R

JPRS 82695

21 JANUARY 1983

USSR Report

CYBERNETICS, COMPUTERS AND AUTOMATION TECHNOLOGY

No. 67

FBIS FOREIGN BROADCAST INFORMATION SERVICE

12
61
AØ4

NOTE

JPRS publications contain information primarily from foreign newspapers, periodicals and books, but also from news agency transmissions and broadcasts. Materials from foreign-language sources are translated; those from English-language sources are transcribed or reprinted, with the original phrasing and other characteristics retained.

Headlines, editorial reports, and material enclosed in brackets [] are supplied by JPRS. Processing indicators such as [Text] or [Excerpt] in the first line of each item, or following the last line of a brief, indicate how the original information was processed. Where no processing indicator is given, the information was summarized or extracted.

Unfamiliar names rendered phonetically or transliterated are enclosed in parentheses. Words or names preceded by a question mark and enclosed in parentheses were not clear in the original but have been supplied as appropriate in context. Other unattributed parenthetical notes within the body of an item originate with the source. Times within items are as given by source.

The contents of this publication in no way represent the policies, views or attitudes of the U.S. Government.

PROCUREMENT OF PUBLICATIONS

JPRS publications may be ordered from the National Technical Information Service, Springfield, Virginia 22161. In ordering, it is recommended that the JPRS number, title, date and author, if applicable, of publication be cited.

Current JPRS publications are announced in Government Reports Announcements issued semi-monthly by the National Technical Information Service, and are listed in the Monthly Catalog of U.S. Government Publications issued by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

Correspondence pertaining to matters other than procurement may be addressed to Joint Publications Research Service, 1000 North Glebe Road, Arlington, Virginia 22201.

50272-101

REPORT DOCUMENTATION PAGE

1. REPORT NO. JPRS 82695

2.

3. Recipient's Accession No.

4. Title and Subtitle
USSR REPORT: CYBERNETICS, COMPUTERS, AND AUTOMATION TECHNOLOGY, No. 67

5. Report Date
21 January 1983

6.

7. Author(s)

8. Performing Organization Rept. No.

9. Performing Organization Name and Address
Joint Publications Research Service
1000 North Glebe Road
Arlington, Virginia 22201

10. Project/Task/Work Unit No.

11. Contract(C) or Grant(G) No.
(C)
(G)

12. Sponsoring Organization Name and Address
As above

13. Type of Report & Period Covered

14.

15. Supplementary Notes

16. Abstract (Limit: 200 words)

The report contains articles, abstracts and news items on theory, design, development and application of analog and digital apparatus, elements and components of control systems, reliability and optimality, information theory, and the theory of automata.

17. Document Analysis a. Descriptors

USSR
Automation
Automata Theory
Information Theory
Computers
Computer Programming

b. Identifiers/Open-Ended Terms

c. COSATI Field/Group 6D, 9B, 9D

18. Availability Statement:
Unlimited Availability
Sold by NTIS
Springfield, Virginia 22161

19. Security Class (This Report)
UNCLASSIFIED

20. Security Class (This Page)
UNCLASSIFIED

21. No. of Pages
59

22. Price

(See ANSI-Z39.18)

JPRS 82695

21 January 1983

USSR REPORT

CYBERNETICS, COMPUTERS AND AUTOMATION TECHNOLOGY

No. 67

CONTENTS

GENERAL

HARDWARE

APPLICATIONS

PUBLICATIONS

COMPUTER PROGRESS AND PROBLEMS IN TAJIK SSSR

Dushanbe KOMMUNIST TADZHIKISTANA in Russian 12 Nov 82 p 3

[Article by Ya. Babadzhanov, director, Tajik branch, USSR State Committee on Science and Technology All-Union Scientific Research Institute of Problems of Organization and Control: "Automated Control Systems Today and Tomorrow"]

[Text] In the "Basic Directions for the Economic and Social Development of the USSR for 1981-1985 and for the Period to 1990" it is written: "To ensure further development and improvement of the efficiency of automated control systems and collective-use computing centers, continuing their unification into a unified Statewide system for gathering and processing information for accounting, planning and control."

No small amount of work has been done in the republic along this line. Improvement of control of the national economy has taken place on the basis of the extensive application of mathematical economic methods and computer technology facilities and the creation of automated control systems. In seven years the computer inventory has increased more than twofold. In recent years mainly improved third-generation computers have been put into service. The most heavily equipped are believed to be the computing center of Gosplan's NIIEMMP [Scientific Research Institute of Economics and Mathematical Economic Methods of Planning], the Ministry of Agriculture ROVTs [Republic Industrial Computing Center], the Tajik SSR Central Statistical Administration RVTs [Republic Computing Center], and the Avtotranssistema Production and Engineering Association.

Within the framework of a comprehensive program, having been developed and being used in the republic are automated systems of planning calculations, of State statistics, for processing information for managing agencies, for standards, for control of science and technology, for handling all-Union classifiers of technical and economic information, for on-line control of quota fulfillment by industry and construction, as well as a number of industrial ASU's [automated control systems]. A republic fund of algorithms and programs has been created. Work has been begun on developing an ASU for the urban economy of Dushanbe.

The development of 147 subsystems is under way and more than 900 problems are being solved in ministries, departments, computing centers and other organizations of the republic. More than 500 tasks have already been introduced in the practice of planning and controlling the national economy. More than 3700 people are involved in developing and using ASU's.

All this speaks for the fact that a definite scientific and engineering base has been created here and specialists have been trained. But problems have also arisen. One of these is the 24-hour utilization of computers. It is still insufficiently high. This is explained by the fact that ministries and departments, having received modern computers, were not prepared to use them in time. And the limited nature of the subject area of problems solved, a shortage of skilled programmers and specialists in servicing computers and the lack of sufficient reserves for the development and use of standard packages of applied programs are not making it possible to bring the utilization up to standard within a short time.

Another problem: Some computing centers and organizations, having been furnished with high-capacity computers, have reduced their attention to the use of low-capacity computers and older models, which has resulted in a reduction of their mean 24-hour utilization.

In the structure of problems solved the percentage of optimization calculations, from whose introduction the greatest savings can be gained, equals a total of about 4 percent. Problems of an information reference nature are being introduced slowly.

It is possible to name other shortcomings, too. For example, many functioning automated systems (as an example, the Ministry of Reclamation and Water Management and Ministry of Agriculture OASU's [automated subject-indexed control systems] officially have not been put into industrial service. Unjustified duplication and independence in working out general-system problems relating to software have taken place. All-Union classifiers of technical and economic information, the unified system of documentation and packages of applied programs are being utilized insufficiently. The reason is non-fulfillment to the full extent of their functions on the part of the republic fund of algorithms and programs, as well as on the part of the system for automated handling of classifiers.

Many ministries and departments have not determined the anticipated or actual savings. Because of this it is impossible to judge the efficiency of measures, although a great amount of money has been put into the creation of ASU's. According to standards, the expenses should be paid back in 3.5 years.

One important shortcoming in the practice of the development of ASU's and the creation of computing centers is the narrow departmental approach. The consequence of this is the origin of computing centers of low capacity and incompatible with one another. It is a good idea to develop a procedure for interplay between an automated control system, centralization of information reference facilities and the economic efficiency of ASU's in non-production sectors of the national economy.

A lack of procedural unification in approaches to developing ASU's for various departmental jurisdictions is felt in all components of the republic automated system. Hence the poor development of planning work and reduction in the level of mastery of complexes of tasks ready to be introduced.

In our opinion it is necessary to intensify coordination of all work relating to the creation of ASU's in the republic and to designate the head performers and customers for all of its subsystems. This will make it possible to concentrate labor and financial resources in the most important directions and to speed up development and introduction of the system as a whole. Know-how can be borrowed from other republics. It is necessary to do this because our Tajik branch of the all-Union scientific research institute, as the head organization for creation of the RASU [republic automated control system], because of limited financing, is not in a position to cover all of the problems associated with the development of general-system materials.

The task of tasks for today, of course, is creation of the Republic Automated System for Controlling the National Economy of the Tajik SSR. It has been entrusted with improving the efficiency of socialist production, raising the level of management of the national economy and of enabling comprehensiveness of planning and control in solving major national economic problems. The RASU will unite automated systems from ASUP's [automated systems for controlling enterprises] to systems for controlling central functional elements.

A comprehensive program for creation of the Tajik SSR RASU has already been developed. It will improve the efficiency of the development and introduction of ASU's of all levels. What is intended? Scientific-procedure and general-system problems will be worked out, relating to creation and functioning of ASU's and ensuring the compatibility of systems. The design and introduction of interindustrial control complexes and of ASU's interacting with them, etc., will be begun.

A positive solution to these problems will speed the development and introduction of automated control systems and computer technology facilities and will improve their efficiency.

8831
CSO: 1863/32

INEFFECTIVE US EXPORT CONTROLS

Moscow DAILY REVIEW in English 8 Sep 82 pp 9-10

[Text] The electronics industry is the most dynamic branch of Soviet industry, writes APN political commentator Gennadi Pisarevsky. In the Eleventh Five-Year Plan period (1981-1985), the USSR will produce millions of microprocessors and tens of thousands of micro- and mini-computers. Soviet plants have successfully mastered the production of superlarge and super-quick-action integral circuits which are as good as American or Japanese. On an area of 1 square millimetre our scientists have learnt to place hundreds of thousands of transistors tied up in a complex electronic device. Their action is measured by thousand-millionths of a second. Our imagination is powerless before such speeds: they can't be either seen or conceived, they can only be used.

The US administration's numerous bans on supplies of computer technology and equipment to the USSR have in fact stimulated the boost of the Soviet electronics industry. It is naive to try to apply "technological racism" against a country that has over 1.4 million research workers and gives a third of the world's scientific output.

Thus, computerisation of work in the USSR now encompasses all branches of the national economy, which are already being served by 5,000 automatic control systems (ACS). Wide-ranging, these systems control technological processes, plants and even whole industries. For example, setting targets for industries alone requires that ACSs and the State Planning Committee perform 10^{16} computing operations a year. That's 10 quadrillions, a number difficult to understand: it is claimed that all people on earth have uttered so many words in all times--since homo sapiens acquired the gift of speech.

The USSR currently has hundreds of computing centres. The largest of them are at the Academy of Sciences, the State Planning Committee and the Central Statistical Board of the USSR.

CSO: 1852/3

CEMA SOFTWARE COOPERATION

Moscow FOREIGN TRADE in English No 6, Jun 82 pp 30-34

[Article by Yevgeniy Mikhailov, deputy general director, V/O Elorgtekhnika]

[Excerpt] In view of the important role informatics has to play in promoting scientific and technical progress, the CMEA member-countries: Bulgaria, Hungary, the GDR, Cuba, Poland, Romania, the USSR and Czechoslovakia have signed an intergovernmental agreement on the development, manufacture and use of computing machinery, and have set up an Intergovernmental Commission (IGC) for coordinating the member-countries' practical efforts to carry out this agreement.

Within the IGC framework, specialized sections of the Economic Council and the councils dealing with the maintenance, and application of computers have elaborated standards defining technical terms, delivery volumes, and support for applied programmes, procedures for package input, etc. for the particular computer installation, as well as conditions for training a user's personnel. All applied application packages are to be supplied to a purchaser in standard form with technical documentation and data media.

At present, in the countries participating in the agreement 137 organizations, including 43 Soviet, are working on application packages. According to the IGC coordinating centre, as of January 1, 1981, several hundred packages were developed and tested in the socialist country.

In 1966 a State Algorithm and Programme Store was set up in the Soviet Union. Developed and tested programmes are also supplied to the Centralized Algorithm and Programme Store of the scientific-and-industrial association Tsentrprogrammsistem, which copies and disseminates packages on commercial terms, and for ordering them it publishes special catalogues and information bulletins. The association's latest catalogue contains brief descriptions of over 200 programmes with a total volume of more than 5.0 million commands.

Moreover, there are such specialized stores in the USSR Academy of Sciences, the scientific-and-industrial association Algorithm and in the computing centres of some industrial ministries and organizations.

The All-Union Association Electronorgtechnica exports and imports software for computer installations.

When exporting Common System computers (CS) and Small System computers (SS), base software, under the technical terms now in force, are included in the set shipped and are taken into account in the price of the computer. Application packages and those intended for expanding an operating system are provided at an extra charge; moreover, Electronorgtechnica organizes installation and the support for the equipment, and also trains the customer's personnel. Soviet-developed programmes are exported to Bulgaria, Hungary, the GDR, Czechoslovakia, Belgium, Finland. For instance, the Institute of Cybernetics of the Academy of Sciences of the Estonian SSR in conjunction with the Elorg-Data firm and with the participation of Electronorgtechnica is now working on a special application package on a separate order from Finalnd's Railway Administration.

The intensity with which computers and, hence, software are used, just as the degree of development of informatics as a whole, characterizes the level which the economic management infrastructure has reached. With the present state of scientific and technical progress the output by the software industry of ever new highly effective programme products will directly enhance the level of the country's industrial production as a whole and actively contribute to the expansion and improvement of the Soviet export programme, thus helping fulfilment of the tasks set by the 26th CPSU Congress for raising the efficiency of social production.

The awarding of the USSR State Prize of 1981 to scientists, designers and leaders of enterprises for the development and the organization of serial production of complexes of the SM3 and SM4 technical and programme facilities as part of the international Small System computers is evidence of the great attention being given in the Soviet Union to the priority development of computing machinery and informatics.

CSO: 1852/4

HARDWARE

NEW SUPERMINIATURE COMPUTERS DEVELOPED

Moscow SOVIET MILITARY REVIEW in English No 5, May 82 p 7

[Text] Soviet engineers have developed superminiature computers which have already found application in the national economy. They are reliable in operation, and speed of computation is 8,000 as high as compared with valve computers, and the functional capabilities 200 times as many. For example, the Elektronika NTs-80-01 microcomputer having a thickness of 2 cm, measuring 30 x 18 cm and weighing 300 g. performs up to 550,000 operations per second and has a large-capacity internal storage.

The new computer uses single-chip superlarge integrated circuits. A thin 5 x 5 mm silicon plate accommodates thousands of transistors, resistors, capacitors, connecting wires.

CSO: 1852/2

SERIES PRODUCTION OF NAIRI-41

Kishinev SOVETSKAYA MOLDAVIYA in Russian 23 Nov 82 p 3

[Article: "Computer Aimed at the Future"]

[Text] Computers today are being provided with a surprising "amount of brainpower" at the Yerevan Scientific Research Institute of Mathematical Machines (YeRNIIM). The latest innovation is the Nairi-41. Series production of it has begun at the "Elektron" Association.

"This is an anniversary for us," says G. Oganyan, manager of the young group of third-generation machine and computer system designers and holder of a Lenin Komsomol prize. "It is the 25th anniversary of service of the first-generation computer, the Razdan."

"The capabilities of the two computers, of course, are incomparable," the young designer continues. "But the institute's first product remains a legend to us. And it is not just the fact that our biography began with it. Incorporated in the Razdan is the collective expertise of Soviet designers from Moscow, Kiev and Minsk handed down to us like a baton. This has allowed the young scientists to undertake in real earnest implementation of a task that is huge in its concept: the integration of computer and communication hardware."

The institute's collective is now engaged in it. Computers developed at the institute are operating in computer centers in the republic and the country, serving entire sectors, planning organizations and industrial associations. The machines developed have unique qualities. Printed in the brochures for many of them are the words: "For the first time in the USSR." Among them is a dual processor system that can execute up to 1,700,000 operations per second.

But now the fourth-generation machines are under development in the design offices. The designs benefit from the input sent here from related laboratories in the country. This creative "ring" that joins the institute together with other scientific centers is making it possible to successfully solve the problem of developing medium size computers with a throughput reaching 5 million operations per second!

8545
CSO: 1863/38

PS-2000 ATTAINS 200 MOPS

Moscow SOTSIALISTICHESKAYA INDUSTRIYA in Russian 28 Nov 82 p 1

[Article by R. Akhmetov (TASS correspondent for SOTSIALISTICHESKAYA INDUSTRIYA), Moscow: "Computer: 200 Million Operations per Second"]

[Text] Based on the fundamentally new PS-2000 computer, the computer system in the geophysical expedition of the "Neftegeofizika" Association has begun operating. Computer throughput is 200 million operation per second. In other words, in the rate of solving a broad range of problems, it is almost 200-fold faster than other domestic machines in operation. The computer concept and design go far beyond ordinary improvements and open a qualitatively new stage in the evolution of Soviet computer technology.

Development of the PS-2000 is an example of close cooperation between science and industry; it is the result of the creative cooperation between the USSR Academy of Sciences, the USSR Ministry of Geology and the Ministry of Instrument Making, Automation Equipment and Control Systems. Scientists and specialists designed the computer in the course of carrying out a major national economic program aimed at increasing the country's proven reserves of minerals, primarily oil and natural gas. But why did the geologists need a computer that processes such a huge volume of information?

Today's prospector is no longer a geologist with a hammer and a knapsack on his back. The search for underground deposits has become an exact science. Here, for example, is how oil and gas deposits are found. Numerous seismographs are set up in a region of suspected deposits. And a seismorecording station is established there. Then several wells are drilled; explosives are placed in them and detonated. The resulting seismic waves spread swiftly throughout the earth's interior. Reflected by various rock interfaces, they rush to the earth's surface where they are recorded by the seismographs. The station records the information obtained by them in digital form on magnetic tape. Judgments are made on the prospects of the region under investigation by the rate the transverse and longitudinal waves pass through the rocks. To check the validity of results of seismic prospecting, wells are drilled. Specialists estimate three productive wells are found for every ten prospecting holes drilled. This is no high rate, considering the large amount of labor and high cost of drilling operations.

"The main reason that geologists have been unable to use a considerable part of the geophysical information obtained during 'illumination' of the earth's interior by seismic waves is that the 'slow' computers available to them with a throughput of a million operations per second cannot process the huge files of information kept on the magnetic tapes of the seismorecording stations," explains V. Kreysberg, head of the department of automated computer systems, Scientific Research Institute of Geophysics, USSR Ministry of Geology, who took part in developing the PS-2000.

The search for gas and oil has to be made under difficult seismogeological conditions and at ever increasing depths. Therefore, the amount of seismic prospecting data is increasing rapidly. And the more geophysical information the geologists get to use, the more precise finding the deposits will become and consequently, the fewer the costly holes that will have to be drilled. This is why the prospectors have great hopes for the PS-2000. It will sharply increase the effectiveness of the country's entire seismic prospecting service and will make a significant contribution to expanding the base of minerals and raw materials and building up the fuel and energy potential in the homeland.

The PS-2000 computer was developed at the Institute of Control Problems, USSR Academy of Sciences, where fruitful work is underway to develop a new class of computers, pneumatic systems for logical control and other devices that facilitate acceleration of scientific and technical progress in key sectors of the economy.

The new machine was developed on the base of the theory of systems with reconfigurable structures that is being evolved at the institute. What does this mean? In compiling a program for traditional computers, a specialist usually "adapts" it to the machine design. But here, it is the opposite. The computer automatically changes the links between its units to solve the problem posed as rapidly as possible.

In every computer, there are usually one or more processors--complex electronic devices that process information. But in the PS-2000, there are 64 processors, interlinked to each other to exchange information. They simultaneously solve one large problem or several small problems.

"The PS-2000 is the first domestic computer that incorporates the theory of reconfigurable structures and parallel distribution of control, which raises sharply its speed and reliability," says I. Prangishvili, deputy director of the Institute of Control Problems and academician of the Georgian SSR Academy of Sciences. "It is oriented to high-speed batch processing of data and is in series production at the Severodonetsk Instrument Plant."

How does our innovation stand up against world computer technology? The Americans, for example, have attained high speed primarily through very high requirements on the technology of manufacture, quality of materials and operating conditions. In the final analysis, this is reflected in the high cost of a machine. But we, the scientist continues, are increasing speed on the basis of a new machine ideology, which is a decisive factor in developing highly efficient and economical hardware. The PS-2000 computer is made with an inexpensive element base and simple manufacturing technology, which has enabled a cost that is not high. Incidentally, the Reagan administration, which has blocked exchanges with the USSR of any information on computer technology, has done this to the detriment of science in its own country. More and more American scientists and specialists justly believe that USSR achievements in the main directions of scientific and technical progress cannot continue to be ignored.

The PS-2000 computer is of course just the beginning. While its information capacity is huge by today's standards, in time it too will be unable to meet the growing need for processing of geophysical information. Scientists at the Institute of Control Problems have already started to improve this model. They intend to bring its speed up to several billions of operations per second.

8545
CSO: 1863/38

APPLICATIONS

AUTOMATED CONTROL SYSTEM DEVELOPMENT FOR VOLGA SHIPPING LINE

Moscow RECHNOY TRANSPORT in Russian No 10, Oct 82 p 24

[Article by V. Chupalov, candidate of technical sciences, VORP [Volga United River Steamship Line] Computing Center: "Ways of Developing 'Parakhodstvo' [Shipping Line] Automated Control System"]

[Text] The automated system for controlling the VORP has passed through several stages in its development, each of which is distinguished by the structure of the problems and the equipment and technology for solving them. At the first stage (1969-1974) the most labor-intensive problems relating to the structure of statistical reporting were solved by means of the "Ural-14D" computer. Input information arrived by mail. At the second stage (1975-1978) information obtained by telegraph was processed on a "Minsk-32". The results were used both for on-line control of the transportation process and for the structure of statistical reporting. At the third stage all problems are being solved on a third-generation computer according to a new technology; using a common information base for on-line and statistical calculations has been provided for, as well as ensurance of the required flexibility of the system for the purpose of timely changing of methods of grouping and outputing reporting data.

In the detailed designs of the PTsB [Shipping Line Central Accounting Office] computing center data were used, relating to the creation of integrated data bases, along with a procedure for solving problems of forecasting transportation operations and modeling the transportation problem on the shipping line scale, and relating to optimization of plans for delivering empty vessels for loading, for automatic control of basing of the fleet by means of computers, and the development of 10-day plans for fleet operations and yearly plans for freightage.

For the purpose of solving the problems of the third stage it is necessary to obtain on-line information on forwarded cargo, and on the basing and state of use of vessels. The existence of this on-line renewable information together with the necessary planning and standards data makes it possible to solve on a computer major problems in controlling the transportation process. However, the problem of gathering from dozens of remote points and inputing into a computer these streams of information is one of the most complicated.

In keeping with the scheme suggested by the PTsB computing center, the shipping line created 29 data processing and computing centers (IVP's) in 14 ports. The IVP is a structural subdivision of the port, which is headed by the senior engineer, to be appointed by the port's director. The main tasks of the IVP are as follows:

providing the VORP ASU [automated control system] with input information; performing computer work for the port's subdivisions by means of the available hardware; and participating in measures relating to a content-rich analysis of the functioning of the shipping line's ASU and improving its reliability and efficiency. The overall program for the 11th Five-Year Plan period called for creation of the ASU in eight ports of the Volga shipping line (except for Gor'kovskiy). IVP's represent the initial structural cell making it possible for ports to train the necessary personnel and to solve all organization problems relating to introduction of the ASU.

Specialists at the VORP computing center revised and created simplified classifier dictionaries for vessels, cargo, cargo processing centers and types of staffs, which had not been prepared in time by TsNIIEVT [Central Scientific Research Insititute of Economics and Operation of Water Transportation], the MRF [Ministry of the River Fleet] main computing center and the PSZB [expansion unknown] computing center.

In February 1981 in Saratov a meeting of IVP personnel was held on the results of use of the data gathering system used for 1980. In additional to organizational shortcomings it was revealed that communications centers did not see to the planned repair and debugging of telegraph sets and to supplying basic materials (paper, punched tape, inked ribbons). Experience has demonstrated that for uninterrupted operation the largest IVP's must have two telegraph sets.

For the information model of the transportation process created with a YeS [Unified Series] computer a letter designation was used for key items of classification, such as vessels, inland waterway points, cargo processing areas, transport operations and cargo. The length of these particulars in on-line messages is from 4-to-6 to 15 characters. These letters occupy from 50 to 85 percent of entries regarding fleet basing; as a result, the length of a single entry reaches 126 characters.

The VORP computing center inputs information into a YeS-1022 computer and checks information received from an IVP. In the preparation of data at an IVP errors are committed, associated with the writing of lettered particulars, such as the designations of points, vessels and cargo. Instead of the designations used in ASU dictionaries, sometimes local designations are used for freight zones and non-general-use wharves, grammatical errors are committed and they do not confine themselves to the established number of characters.

VORP computing center personnel constantly analyze errors, give recommendations and improve ASU dictionaries, adapting them as much as possible to traditional methods of abbreviating names of cargo, vessels and stations.

The length of telegrams for IVP's of various ports varies from a few lines to 100 to 130 (10,000 to 13,000 characters). The probability of error-free reception is reduced with an increase in the length of a telegram. Therefore, it has been deemed advisable to break up a message into parts of 15 to 20 entries and to transmit them over several communication sessions. The use of digital codes makes it possible to shorten on-line messages twofold and to improve their reliability.

The computing center is now at the stage of re-equipping, of converting to a new data processing technology for statistical calculations, and of the creation of the organizational foundations for solving new problems in on-line control of the transportation process. Under these conditions the center's team has to issue statistical reports within the established deadlines and at the same time to form reference data and to prepare machine media for initial data for working according to the new technology.

The lack of internal hardware for rapidly correcting errors detected, as well as an insufficiency of machine time, have not made it possible as yet to process totally all the information and to obtain reliable and complete data. A building with a total area of 1000 square meters is being constructed at the shipping line for the purpose of installing new computers and other equipment. Plans have been made to put into service a YeS-1035 computer, a teleprocessing system with eight video monitors and four user stations, and a YeS-9003 system for preparation of data on magnetic tape. The presence of this equipment will make possible normal functioning of the system for on-line gathering of information on the course of the transportation process within the range of the shipping line, and the solution of the problems provided for by the coordination plan.

Long experience in relations with the PTsB computing center has demonstrated that a production center must have its own specialists for formulating problems and developing detailed assignments. The customer (the steamship line) must be ahead of the designer in formulating problems and developing the general methodological and technological principles for solving them and thus specify the general direction for development of the ASU. In order to meet these requirements and be an active client not only at the stage of receiving programs (when major alterations are already impossible), but also in the course of the detail design, the shipping line's computing center must have its own ASU division with industrial-engineer problem formulators, specialists in software systems and programmers who would be able to utilize know-how gained in the course of industrial use of the ASU and to constantly modernize programs. The PTsB computing center does not have the ability to introduce sufficiently efficiently changes in existing programs.

The once necessary and progressive division of the industrial ASU at the port - - steamship line - ministry level has clearly become obsolete at the present time. The boundaries between ASU levels are vague and further specialization of the computing centers of the PTsB and PSZB and the main computing center with TsNIIEVT has presented many difficulties to designers in coordination of design solutions. More progressive at the present time is specialization with respect to through subsystems or groups of close subsystems. The time has come to create a scientific research and design organization for ASU's which is unique for the entire industry. This is one factor in raising the scientific and technical level of designs and the efficiency of automated control systems in river transport.

8831
CSO: 1863/31

CENTRALIZED COMPUTERIZED ACCOUNTING FOR RIVER FLEET

Moscow RECHNOY TRANSPORT in Russian No 10, Oct 82 p 25

[Article by N. Davydov, chief accountant, Amur Shipping Line: "We Solve Problems by Means of Computers"]

[Text] "Mechanization of Accounting--Major Objective"--an article from the work experience of the team at the Northwest Shipping Line's Leningrad port was published under this title in RECHNOY TRANSPORT, No 5, 1982. We are publishing readers' responses to this topic.

Scientifically validated planning, efficient good use of finances and reliable accounting should be conducive to fulfillment of State plans and quotas with minimum input and high efficiency.

Reliable accounting and reporting are necessary conditions for proper evaluation of the fulfillment of production and financial quotas by enterprises and of the introduction of cost accounting. As the economic control mechanism develops and is improved accounting should become less labor intensive and more accessible to a wide range of personnel, be easily subject to mechanization and automation, and be efficient. The existing organization, approaches and methods of conducting accounting still do not meet these requirements to the full extent.

The mechanization and automation of accounting by means of computers should play an important role in improving the efficiency and quality of accounting. The use of computers orders the accounting system, imposes heightened requirements on primary accounting documentation and raises the work of accounting and bookkeeping personnel to a qualitatively new level.

In mechanizing accounting, difficulties arise in development of detail design documentation, for which considerably more time is required than for the development of the same documentation for punched card machines, as well as a broader range of specialists.

Experience has demonstrated that the development of plans for mechanization of accounting using a computer for a single or several shipping line enterprises is economically unfeasible. Therefore, detail design documentation must be developed on a centralized basis and be acceptable for introduction at all MRF [Ministry of the River Fleet] enterprises.

Many inconveniences are experienced by newly organized computing centers and machine calculating stations (MSS's) whose possibilities for programming are limited because of the fact that many shipping line computing centers have been furnished with various types of computers and the programs for them are written in various machine languages and at various levels. For example, the MSS of the Amur River Shipping Line created in 1976 was furnished with two sets of alphanumeric punching equipment. In six years of operation total mechanization of accounting was carried out mainly at the shipping line's enterprises located in Khabarovsk.

The limited capabilities of punched card computers for total mechanization of accounting have resulted in the fact that now at the station accounting documents are processed on four types of machines. Documents for accounting for stores and supplies and for accounts with suppliers are processed on a "Minsk-32" computer, for labor and wages accounting on a YeS-1022 computer, and accounting for fixed capital, financial resources and accounts is performed on a punched card computer and a small M-5010 computer.

The small M-5010 computer was put into service in 1981. Preparatory work was performed in advance for the purpose of solving problems on the new machine. A programming department was set up at the shipping line's MSS in 1979. It took three years to select and train specialists for the newly created department. Now eight programmer-engineers work in the programming department and five of them have undergone retraining at Vilnius Institute for Improving Skills. At the same time plans for mechanizing statistical and accounting calculations have been developed and introduced. In 1982 complexes of problems are being solved on the M-5010 computer relating to accounting for all kinds of the fleet's work with the issuing of monthly, quarterly and annual statistical reporting forms, and a project for mechanizing statistical reporting on the utilization of the transport fleet is being developed and will be introduced.

Accounting for fixed capital and crediting of amortized expenditures, accounting for financial resources and settlements, and compilation of a synthetic report have been mechanized. All this made possible utilization of the M-5010 computer for a single shift, and by the end of the year the daily demand for machine time will increase to 15 to 18 hours.

Three generations of computers were replaced in the last 15 years. This is normal, but the process of mastering and introducing them has lagged behind considerably because of a lack of ready unified programs, especially for mechanizing accounting. Therefore, it is necessary that management of the development and the development itself of unified programs for mechanization of accounting for future types of computers be carried out by the MRF's main computing center. The existence of ready programs will considerably speed the process of total mechanization of accounting in river transport.

A very important measure for improving accounting is the creation of centralized accounting offices at major water transport centers of shipping lines. This improves the quality and reliability of accounting and reduces the number of accounting personnel.

The creation of a centralized accounting office and the use of computers for processing primary accounting documentation will considerably improve the efficiency of accounting and will improve preliminary control of the consumption of material and financial resources. Especially strict control must be established over the consumption of fuel, materials, spare parts and other assets. A considerable role in this must be played by a scientifically validated standards base, which still does not exist in shipping lines.

If a certain amount of work has been done on standardizing the consumption of fuel in shipping lines, consumption standards have not been established for the consumption of other kinds of raw material and materials, and preliminary control does not ensure their economical and careful use. Problems relating to the development of standards for input of materials for maintaining the fleet and for transferring equipment and repair work require their own solution.

The organization of centralized accounting will make it possible more efficiently to solve problems relating to financing all the operations of enterprises, since in this case considerable concentration of financial resources is made possible.

According to the plan, in 1985 a centralized accounting office is to be created which will serve six shipping line enterprises located in Khabarovsk. Even now the mechanization of accounting is being carried out at these enterprises according to unified plans, and in 1983 the total mechanization of all accounting divisions will be completed.

The centralized accounting office must be assigned space and motor vehicle transportation for uninterrupted communication with enterprises and for gathering primary documents. To the staff of the centralized accounting office must be added two or three highly skilled specialists in analyzing the financial and economic activity of enterprises.

According to preliminary estimates, the creation of a centralized accounting office in Khabarovsk will make it possible to release not less than 10 accounting personnel and will improve considerably the quality of accounting and reporting.

At the present time the shipping line's MSS is no longer coping either with the work volume or with the tasks associated with development and introduction of an automated system for controlling river transport at the shipping line level. We hope that with the receipt of a second M-5100 [as published] computer the MRF will solve the problem of creating in the Amur Basin a computing and data processing center which will make it possible to solve with higher quality all problems relating to the introduction of mechanization and automation in control.

8831
CSO: 1863/31

PROTECTING INFORMATION IN COMPUTER SYSTEMS

Moscow NOVOYE V ZHIZNI, NAUKE, TEKHNIKE. TEKHNIKA. ZASHCHITA INFORMATSII V VYCHISLITEL'NYKH SISTEMAKH in Russian No 6, Jun 82 pp 3-59, 64

[Booklet "Protecting Information in Computer Systems" by Boris Mikhaylovich Rudzitskiy, Izdatel'stvo "Znaniye", 43520 copies, 64 pages]

[Text] Reviewer: V. O. Bondarenko, candidate of engineering science.

Boris Mikhaylovich Rudzitskiy is a candidate of economic science. He is the author of more than 30 scientific works, including two books and two booklets. His scientific and writing interests include the problems of practical application of computers in managing the national economy.

Considered in this booklet are the problems of safeguarding the security and integrity of information in computer systems. Described are software, hardware, organizational and cryptographic ways and means of ensuring the safety of data at all stages in automated processing.

This material is intended for specialists in various sectors of the national economy, lecturers, students at people's universities, propagandists of new technology and students in technical VUZ's.

To the Reader

Practically in any book dealing with the problems of data processing in computers and systems, one can find chapters related to one extent or another to the problems of protecting information. This is no coincidence. The functioning of a modern computer system is inconceivable without a thorough and profound critical analysis of them.

The intensive development and production of computers has compelled approaching the problem of protecting information in a new fashion. Earlier, for example, a code was considered highly reliable and safe when it was believed that it could not be broken manually within a 100 years. But modern methods of cryptanalysis coupled with parallel processing of information on high-throughput computers allow breaking it within just 24 hours. In other words, the concentration, specialization and integration of information in a computer offer significantly more advantageous conditions for obtaining information previously inaccessible.

Computers are now used to process planning, economic, statistical, demographic and other information of a global nature. The number of computers and the area of their use in managing the economy and its sectors is expanding considerably. Any complex system requires setting up electronic systems commensurable with the problems to be solved. But the value of the data is directly proportional to the preservation of it, to the protection from garbles, destruction, loss, etc.

There is a huge aggregate of information that is collected, processed, stored and transmitted over communication channels. It is well known that the volume of data circulating in society is doubled on the average every five years. And along with the increase in volume, data access methods are expanding, and fundamentally new ways and means of obtaining it are emerging. Here one can cite primarily intelligent terminals, distributed data banks, laser communication and other promising means of user communication with computer systems.

There is continual improvement in the architecture of computer systems, and in their systems and applications software, hardware and information base. The new element base and achievements in multiprogramming and multiprocessing complicate organizing the protection of information in computer systems. Consequently, the need arises to reexamine approaches to implementing protection, enhance its effectiveness and achieve high quality in operation.

On the other hand, research in computer architecture, programming, cryptography and other related disciplines allows developing reliable and highly effective methods, means and measures for protecting information.

Protecting information is a multiaspect concept. It can be approached from the interests of users, programmers, operators, servicemen and administrators of computer systems. Accordingly, the instruments of protection have to be separated. But common in organizing it is the systems approach, i.e. the necessity of using it at all stages of the process of converting data in a computer system.

This booklet on the state and problems of organizing protection of information in computer systems in the developed capitalist countries attracts interest by the presentation of material precisely from the systems viewpoint. In an interesting manner, the reader will learn of the main threats that occur during the functioning of computer systems as a whole, as well as individually at the stages of data processing, transmission, storage and input/output. The description and classification of protection system components is substantial. It is important that the relationship is shown between the threats that occur and the methods of defeating them.

While dwelling in detail on the problems of protection, safety and integrity of information in computer systems, the author strives to bring out all aspects of each question by using a large number of examples. The interrelation between the various components of a protection system at each of the data processing stages is considered distinctly.

The chosen form of presentation allows a coherent and logical transition from the description of protecting data security to protecting integrity and vice versa, and in doing so covering the most essential design solutions. Accenting the description of largely the hardware, software and methods of protection enables the reader to become familiar with the engineering implementation of protection systems. And finally, drawing on examples of organizing protection systems gives a clear idea of the achievements made here.

The content of this booklet allows concluding that protecting information involves many sciences. What is especially important in this connection is that the author has succeeded in subordinating the presentation to a single goal: an examination of protecting information as a discipline of its own.

It is important to note that many aspects of protecting information are not typical or characteristic of our country and those that are members of the CEMA. They are, rather, of cognitive interest. But covering them is sound and expedient for readers to become thoroughly familiar with the problem.

V. I. Maksimenko, doctor of economic science, department chief, Main Administration for Computer Technology and Control Systems, USSR State Committee for Science and Technology

Data Security and Integrity, by B. Rudzitskiy

Where and What to Protect. Attempts to keep secret the content of messages, negotiations and records have a history going back many centuries. We know about methods of encoding information back in ancient Egypt, ancient Rome, in the Middle Ages, etc. Leonardo da Vinci, for example, wrote down his thoughts in such a way that they could be read only by using a mirror. The well-known, seventeenth century English philosopher and statesman, Francis Bacon, described methods of encoding information in "De Augmentis et Dignitate Scientiae" [The Advancement of Learning]. Many such examples could be cited.

In a broad sense, protecting information has ethical, legal, social and other aspects. But they are all subordinate to a common goal: controlling the security of information in managing a particular firm or economic association.

An immediate explanation is called for here. Readers who do not specialize in protecting information must unequivocally appreciate that protecting information from intentional distortions, unauthorized users, criminal situations, i.e. protection of security, is only one aspect of the matter.

These problems, of course, require their own solutions. But the concept of "protecting information in computer systems" itself means the ways and means of functioning of these systems under specified conditions with the impossibility of both intentional and accidental disclosure, change and distortion of data.

From the aspect of protection, the following basic requirements are imposed on data processing in computer systems. Work with information must be controlled and recorded from the time of entry into the system to output to users. There must be the capability for restoring and recovering data when it is accidently distorted and (or) tampered with. It is important to ensure a reasonable compromise between the effectiveness of protection against hardware and software failures, accidents and intentional destruction on the one hand, and deterioration in time and cost characteristics of operations on the other (complexity of access, extension of processing time, system bureaucracy).

A scientific approach to organizing protection of information has recently been formulated. In a number of Western countries (the USA, Japan, FRG, etc.), special journals devoted to various aspects of protection are published. Problems of implementing protection systems on specific computers are included in the computer personnel training program. There are sections on the theoretical and practical problems of keeping information safe in computer systems at scientific conferences. It is well to begin the description of the facilities, methods and measures of protecting information with a definition of the main concepts of the problem in question as well as with a classification of possible threats.

The concept "protection of information in computer systems" assumes the performance of studies in two mutually related directions: data security and data integrity.

Data security concerns protecting information from intentional destruction and distortion or accidental access to unauthorized users. Such users could be both personnel working with the computer systems and outside personnel and organizations.

Data integrity, however, is the guarantee of data consistency, correctness and completeness. Users are given the right to communicate with the computer system, i.e. they are authorized and not accidental.

For presentation clarity, two other concepts have to be unequivocally defined: "secrecy" and "confidentiality." Secrecy is the level of authority granted to organizations and users to implement acquisition, processing, storage, transmission, application and dissemination of information among other users and organizations. There is a connection between secrecy and security. But secrecy, as a rule, is considered outside the computer system. This is because of the need for taking special measures to maintain secrecy, for example, of a legislative nature, that do not infringe on the activity of computer systems.

Data confidentiality is the status of data. It is specified by an organization or person and determines the required level of information protection (the measure of correspondence between the value of the information to be stored and processed and the costs for design and implementation of the required level of data protection).

Let us stress that information integrity must be absolute, i.e. the users interacting with the computer system must be confident of the correctness, consistency and completeness of the data and the relations between it. But security is relative, inasmuch as it is practically impossible to fully protect information from unauthorized access.

There are many aspects to classifying the threats to information security and integrity in computer systems. Let us isolate the following basic directions in threat classification: by type and degree of vocational training of operators, programmers, users, etc.; by type and location of occurrence of violations; and by frequency of attack and the cost of damage caused.

Potential violators generally include programmers, operators, administrators, users and servicemen, i.e. the people officially authorized to communicate with a computer system. However, when such people exceed their authority and (or) commit illegal actions, they become persons intent on doing damage without the right of interacting with the computer system.

To determine the ways and means of protecting information, it is useful to distinguish the level of training of violators. By degree of training among violators, there may be low-skilled, skilled and highly-skilled personnel. Consequently, the level of training of violators is inversely proportional to reliability and directly proportional to the complexity of protecting information. Also, the most complex protection is that against highly skilled personnel officially authorized contact with the computer system.

The type and location of occurrence of violations is largely determined by the type of violators. A serviceman, say, may disconnect hardware for computer protection; a programmer may disable a program for protecting stored data; a user may request unauthorized data from terminals, etc.

From the aspect of violating security and integrity, types of violations accordingly are subdivided into intentional and unintentional. Intentional violations include tampering with (destruction of) data media from the territory of the computer center, interception of communication lines during data transmission over channels, unauthorized copying of data by using terminals and others.

Distortion of integrity is the result of accidental personnel mistakes, incorrect execution of programs (erasing of data, blocking, ineffective management of jointly processed data), etc. A special place is held here by natural disasters, for example, fires, floods, explosions.

The frequency of onset of damage is inversely proportional to its cost. According to foreign data, the frequency of onset of damage valued at less than one dollar is several dozen times per day. And conversely, there are unique cases when aircraft have falled on computer centers causing losses of tens of millions of dollars,

In a number of cases, it is not difficult to determine losses since the price of a copy of stolen information media or stolen hour of computer operation is well known. However, it is not always possible to unequivocally establish the cost of recovering distorted, erased and stolen information due to indeterminate complexities in restoring and acquiring it.

Specialists believe that the damage from stolen and unsound data is considerably higher than that from stolen equipment, maintenance documentation, etc. And finally, as a rule, only one percent of data protection violations in computer systems are discovered. This indicates that damage estimates are low and that the frequency of occurrence of threats to information security and integrity are higher.

Threats to information security and integrity exist at all stages in the process of data acquisition and conversion in computer systems. To determine measures to protect data in a system as a whole, let us examine methods of violating security and integrity that exist in practice in each stage of the process. And let us stress once again the irrelevance of some aspects of this problem for socialist society.

When users interact with a computer system at the input (output) stages, external peripherals, primarily terminals, are subject to the main risk. From terminals, one can illegally copy information and enter data known to be false. For this purpose, unauthorized users are masked as valid, terminal radiation is recorded, and the display screen is observed visually. Threats to integrity include input of erroneous information and (or) its output through I/O channels with an incorrectly specified number.

In a number of cases, issue and input of erroneous information occur as a result of conventional negligence. For example, an operator forgets to disconnect a terminal, or a user is not very familiar with terminal operating instructions.

Electromagnetic radiation occurs while a computer is operating, i.e. the computer is a data transmitter. Special equipment can be used to intercept and decode this radiation. Directed external radiation also has an effect on a computer; it can cause the computer to malfunction and distort the data being processed.

There is also the danger of intentional malfunctions in the protection software and hardware in the central processor and main storage unit. As a result, dynamic allocation of processor resources is upset, unauthorized access to data files in main storage occurs, control over location bounds ceases, and unauthorized reading of information occurs.

Foreign specialists note that cases of information theft make up about a third of all crimes in computer centers. Protection against theft is complex, laborious and not always sufficiently effective.

The threat to integrity during transmission over communication lines includes data garbling when it passes over the channels, erroneous switching, crossfire and similar inadvertent violations. The main ways of violating security here are interception of the electromagnetic radiation in the communication lines, illegal seizing of information during long-distance transmission of it, intentional disruption of a communication line and connection to them. When a connection is made, unauthorized users can listen in and copy messages being sent and make false insertions in them (add information distorting the message).

Let us put into a separate group those threats pertaining to the process of information acquisition and processing in computer systems as a whole. They are extremely difficult to predict and it is extremely difficult to organize appropriate protection against them. These are the unfortunate incidents and natural disasters: floods, fires, earthquakes, etc.

Thus, information has to be protected from threats to its security and integrity: when data is transmitted over communication lines, during disasters and accidents, in the process of data conversion in computers, during data I/O.

In organizing protection of information sent over communication channels, do not allow those intent on doing harm connection to communication lines and equipment; especially secret information should be shielded; prevent the possibility of interception of electromagnetic radiation; prevent the mutual effect of communication lines and the effect of electromagnetic fields on them; and achieve the required completeness, validity and accuracy of the data being sent.

Protection against accidents and disasters calls for strict adherence to fire prevention rules; do not tolerate cases of violation of work and production discipline; observe equipment operating rules; substantiate the location of the computer center site.

To protect data during processing, prevent the interception of electromagnetic radiation; organize the proper, coordinated and controlled operation of users, equipment and software for data conversion in computers; do not allow mistakes in the activity of personnel servicing computers; prevent penetration of external radiation into the machine room; and keep track of the use of CPU time.

To protect information during storage, prevent cases of wrongly giving out media from the library; prevent theft and distortion of information on media; ensure the required conditions for keeping and maintaining information; and provide additional shielding for especially secret information.

During computer data I/O, protection comes down to catching and correcting input errors, preventing unauthorized users from using terminals, preventing interception of electromagnetic radiation, adhering to instructions for operation of peripherals, determining and eliminating cases of wrongly outputting information.

Protection against these threats is implemented by the protection system (SZ). This is the aggregate of facilities, methods and measures organized and maintained to prevent destroying, receiving or changing protected information in a computer system: the hardware, software methods, organizational steps (measures), and cryptographic methods (protected conversions). The protection system functions under control of a special and authorized administrative protection team.

Various components of the protection system are used as a function of the threat against which protection is required. For example, cryptographic methods are used as a rule in data storage and transmission. Protection fundamentally has a high priority. Thus, protecting the computer system as a whole has a higher priority than restricting access to information files.

Protection systems being designed and in effect vary by composition, principles of organization and operation, effectiveness and other ways. The basis of the variation is the functioning of the computer system, the nature of the environment, and user requirements. A set of protection systems can, however, be subdivided into a number of subsets based on the functional characteristics of the protection system, i.e. each subset supports a specific level of protection.

At the first level, there is no protection. The computer system, consequently, is open to both authorized users and to those intent on doing harm. In this connection, the value of any threat increases sharply and the resistance to security and integrity violations is sharply reduced.

Computer system protection increases when users are completely isolated from each other with respect to information (the second level). Each user (group) interacts with just his own data files. There is, however, a small amount of common information, say a library of standard routines.

A third-level protection system takes into account a user's right to access data files. A user list is drawn up; each one on the list is granted permission to work with a specific data file (reading, writing or execution if the file is a program). In contrast to the preceding level, here the users are not isolated and the accent in implementing protection is placed on the organization of its unified scheme. Practical development of such protection systems is complex. Functional properties of the protection system are expanded and users are given the capability of controlling access to their data and programs by various methods (by software, as a rule).

For example, users specify that only programs in a specific set can have access to the set of data and program elements. And protection is enhanced by individualizing and specifying locations of access to programs. In other words, they conclusively determine access to protected information. Another example of control: users set the time of access and (or) bounds for changing values of an element within which it is enabled.

At the latter level, a fundamental feature of protection is the control not only over conversion of data in the computer system, but also over subsequent use of it. Subsequent (after the data is output from the computer system) access authorization is achieved, for example, by assigning the appropriate secret classifications. Let us note that such control is largely local and not often encountered in a protection system.

The major principles of development of a protection system include: simplicity of the protection mechanism, openness of design and operation of the protection mechanism, naturalness of the protection system, completeness of control and recording of violations, restriction of capabilities and distribution of functions of users, and restriction of common protection system components.

Protection system simplicity is a major principle in system design. Experimental testing does not always bring out the "bottlenecks" in protection system components. Industrial operation alone allows determining all the shortcomings (access paths not considered, long time of response to violations, low reliability, etc.). Timely elimination of shortcomings requires thorough testing of each component in the protection system. This, in turn, requires simple and clear implementation of the protection system.

Protection system reliability must be invariant to the training level of violators. Thus, the general concept of protection mechanism design must not be secret. Weak points in the protection system are easily and quickly brought out when it is widely discussed, say, in scientific publications and at conferences. However, information affecting user interests (passwords, keys, etc.) should not be revealed and the capability of destroying the protection mechanism, the operational essence of which is known, should not be allowed.

In foreign practice, a protection system is considered effective when a description of it can be published in the open press. In this case, it becomes for the user psychologically more attractive, reliable and effective.

User interaction with a protection system must be natural and simple. Using unusual methods makes it psychologically unattractive. As a result, users try to avoid adhering to the protection system operating rules, which results in a large number of errors. A rational approach here is standardization and unification of user interface with the protection system.

The principle of completeness of control and recording of violations means comprehensive and continual checking of each access to the computer system as well as recording of attempts at unauthorized penetrations.

Through access control is a major protection system function. Users must be guaranteed protection of security and integrity of information even when there are errors in the protection system. Changes in user privileges must also be taken into account, i.e. dynamic control is required.

Since it is practically impossible to prevent leakage of information, recording attempts at unauthorized penetration of the computer system is suggested as the only alternative for developing reliable protection systems. This aids in timely detection of a violation of protection and taking steps to restore it. It is difficult to record unauthorized actions, especially when there are malfunctions in the protection system. It is therefore advisable to supplement recording of violations with modeling of actions of unauthorized users and simulation of errors in the protection mechanism.

A sharp reduction in time and cost of detecting protection violations results from restricting "superfluous" user privileges. They raise the probability of accidental and (or) intentional errors. Thus, in designing a protection system, the people interacting with the computer system should be furnished (their programs, resources, etc.) with the minimum authority that still, however, enables performance of the productive functions.

Distribution of functions enhances protection reliability and offers additional capabilities for choosing its directions. It is essential to separate access tools, say, keys, between users, i.e. to logically and soundly isolate the tools for interaction with a computer system. This results in the capability of combining the conditions of access to information and consequently of increasing the number of protection strategies.

And finally, the last principle is restricting the number of common protection system components. Protection parameters within the system itself that are common to users, say, the number of common information communication lines in the protection system, have to kept to the minimum. It is difficult to implement this in practice since such parameters must meet the interests of each user. Also, maximum separation of component protection increases protection system response time considerably. It would be effective to provide in the protection system for the capability of combining isolation of unified characteristics in the "system part" of the protection mechanism with their inclusion in the "user part," i.e. combining the interests of both the users and the protection system.

How to Protect. There are a large number of methods, means and measures for protecting information in computer systems. Software protection methods have been implemented in the form of the following basic sets of programs: identification of equipment, users and files; prescription of rights of equipment and users; protection of files of data, operating systems and user programs; auxiliary functions (control of protection mechanism functioning, blocking of passwords, etc.); and protective conversion of information.

Information protection programs should be included in the computer system software in the form of a software package that offers simplicity in expanding program modules and universality of them.

A basic difficulty in hardware protection of a computer system is the territorial distribution of its components, as well as the multimode operation of a computer (time sharing, multiprogramming, multiprocessing and others). Based on specific features, protection hardware is made both as standalone equipment and as built-in in the computer system hardware.

In series production abroad are electronic-optical, electronic, electronic-mechanical, mechanical and other protection hardware: registers containing protection system attributes (secrecy classifications, passwords, etc.); descriptor registers for controlling the bounds of computer main storage; switches for protection of external storage; devices for identifying users by individual properties; bits for the privileged state in central processors; generators of codes identifying devices in computer systems; circuitry for implementing protective conversions; and special storage units for storing protection programs.

Organizational measures are used to protect against almost all known violations of security and integrity in computer systems. This includes organization of observation in a computer system; testing and training of personnel (users); construction of structures for protection against disasters and unauthorized access; monitoring changes in systems and applications software; creation of a special, administrative protection team; establishing pass checkpoints; and drafting of standard regulations on activity of the computer system and the protection system.

Crytographic methods of protecting information are the only way of safeguarding it from unauthorized access during transmission over communication lines. They are used also in storing data and in user identification. They are implemented in computer systems by hardware, software or a combination of both.

Applying these methods in computer systems calls for rather diverse ciphers that will allow "shielding" information by various methods: character substitution, character transposition, analytic transformations.

Let us make some conclusions. Effective information protection is possible only on the basis of full use of each protection system component discussed. Second, in choosing data protection methods, one must consider the relationship between time and cost spent on implementing them and the losses from distortion, destruction and theft of information.

Input and Output Protection. User "authenticity" (and sometimes his rights) must be established in all cases of user access to a computer system. When users receive results, the authenticity of the computer system (terminals, computer, etc.) must be established. Maintenance of data security and integrity and the I/O process must be guaranteed.

The main means of protecting access is user authentication: his identification and establishment of authenticity. This is done by assigning unique, nonrepeating names and numbers to a user or, say, a terminal. They are subsequently used to identify and account for the number of accesses to computer system resources.

Identification alone, however, is insufficient for determining access authenticity. The user has to also prove the validity of his identification. The following procedures are used in a protection system to confirm the authenticity of users and elements in computer systems: presentation of passwords or passwords together with a secret code; organization of dialogs; implementation of a conversion function; checking of individual characteristics; and implementation of a physical connection.

Authenticity may be confirmed not only at the initial access, but several times, which enhances protection reliability. This is done, for example, in the following procedure: user request input; identifier request; identifier check; when response is positive, connection of procedure for checking authenticity; and when the user has been successfully identified, permission to work with the computer system.

As a means of confirming authenticity, passwords are used practically in any effective protection system. A password is a set of alphanumeric characters with specific parameters: time of validity, length, method of obtaining, form of assignment and others.

By time of validity, passwords are divided into those without an effective restriction and those used within specific limits (password life cycle). Extension of the limits is inversely proportional to password reliability and its protection against someone accidentally or intentionally figuring it out. On the other hand, frequent replacement of them entails considerable organizational difficulties and time (especially on letting users know).

Password length is the number of characters in it. In computer systems, the length, as a rule, is from 4 to 18 alphanumeric characters. Length is a basic characteristic determining the protection of the password against regular attempts to discover it. The number of characters in the alphabet from which the password is built must also be taken into account. A large number of characters in the alphabet together with extended length enhances reliability and expands the range of application of passwords.

Passwords are obtained in two ways. In the first, users themselves choose the combination of characters based on convenience and simplicity of remembering them. These passwords are difficult to forget and need not be recorded. But they are easy to figure out; therefore, it is advisable to complicate the combination of characters. This leads to the need of recording them and thus increases the probability of them being obtained by unauthorized users. Protection against unauthorized obtaining of them comes down to, for example, adding spaces in the password text. This is rather reliable since only the authorized user knows the actual number of spaces.

The second method entails deriving passwords through protection system facilities. The system includes a random word generator that forms easily pronounceable syllables that are then combined into passwords. The principle of operation of the generators has been described in the literature. Only the algorithm by which the passwords are formed need be protected. The advantage of this method is its immunity to attempts to discover it.

A promising direction in assigning passwords is to build them into computer system devices. This is especially important for access protection. Thus, the password has to be keyed in first through the keyboard to switch on a terminal with a built-in password. Otherwise, the terminal will not be connected to the communication line.

Authenticity is confirmed by using passwords as follows. The passwords are stored in computer, terminal or other storage from which they can be interrogated by the protection system. The user keys in his identifier using the terminal keyboard. It becomes the argument for the protection system, i.e. it is used to select a password from storage. This password is compared to that entered by the user from the terminal. If they match, the system proceeds to the second phase of access protection: checking the right of access to protected elements in the computer system. When there is no match, the terminal is disconnected, an alarm signal is triggered (audible or light), and the protection system administration is notified.

An interesting solution would be to accept continuation of work with a user who had not confirmed his authenticity. After "verification," the protection system intentionally deludes him while gathering information on the nature of the queries. Then this information helps identify the unauthorized users and improve the protection mechanism.

Establishing authenticity by using passwords and a secret code is essentially an evolution of the procedure with ordinary passwords. A password and various characters of a secret code known only to the user are specified. The number of characters and their position in the code system are determined by the protection system by using, say, a random number generator.

A secret code enhances the effectiveness of access protection. First, discovery of the individual code characters does not rule out the possibility of subsequent use of the code. Second, it is difficult to obtain the secret code as a whole. And third, interception of a password does not necessarily mean access protection is violated.

The password is a major element in a protection system. Access protection reliability as a whole depends on password security. In this connection, special attention has to be paid to password security and integrity. Studying the practice of protecting passwords in computer systems has allowed formulating the main principles.

Password security must be provided for when they are created, distributed, stored and transmitted over communication channels. When a password is entered from a terminal, the print mechanism must be disconnected and no text displayed on the screen. Some terminal models to not provide for disconnecting the mechanism. In them, passwords are blocked or masked out by other symbols (dark pattern in the form of squares connected by lines). When the information is output, say, on an alphanumeric printer (ATsPU), a special routine inhibiting password printout is required. Passwords can be stored and transmitted over communication lines only in translated (encoded) form. A more reliable method of disseminating them is to deliver them in person and to obtain a signed receipt from those responsible for protecting them. All cases of use of passwords should be recorded. From time to time, a valid user compares the log with his own data. If there is any discrepancy, a protection violation is recorded and the password changed.

Another procedure for confirming authenticity is the organization of dialogs. Checked in them are answers to standard and (or) individual questions concerning, as a rule, the "personal life" of a user. A list of questions and answers is stored in computer storage. The protection system interrogates the user and compares his answers to those stored in the computer. A complete match of all answers enables access.

In computer systems with a large number of users, the dialog should be oriented primarily to standard questions. The result is a considerable savings in storage for the list content. Examples of standard questions are: "What year were you born in?", "What is your last name?", etc. Examples of individual questions are: "Give the names of your children;" and "What is your mother-in-law's middle name? [patronymic]."

Dialogs are a reliable means of confirming authenticity. The drawback is their length, which is especially inconvenient in computer systems with multiaccess.

An evolution of dialogs is found in conversion functions. The user enters an identifier from the terminal; in response, a random number generator outputs a pseudorandom number to the user. It is converted by an algorithm known only to the user. In turn, the protection system program performs the same conversion. Results are compared and if they match, access is permitted.

Here is an example to help explain the concept. Assume the pseudorandom number "1950" is output upon inquiry and transformed by this algorithm: add the even and the odd digits in the number, respectively; multiply the sums; and then add the day's date (say it is 26; it can be generated automatically everyday). Then $(1+5)X(9+0)+26=80$. Thus, access will be enabled if the number "80" is formed by both the protection system and the user.

A feature of this procedure is its high immunity to discovery. Suppose the result formed is intercepted by some unauthorized person. The maximum gain that the unauthorized user can extract in this case is the attempt to break the intercepted text. A mathematical estimate shows that it is impossible to uncover a complex conversion algorithm. Thus, there is no need to store a password in the computer system or for the user to have one. Protection of information against threats to integrity, created by authorized users, becomes effective since different conversion functions are assigned to them. The only problem is that a user may forget an algorithm. In this case, he will not be able to recover the right to access on his own and will have to turn to the administrators of the protection system.

The next procedure is a check of individual characteristics. Every person has different fingerprints, voice patterns, etc. There are now devices to confirm authenticity by recognition of voice audiograms, fingerprints, head shapes, odor, etc. As a rule, they are built into terminals. Thus, the process of identification and establishing authenticity becomes unified, i.e. the need for user identification is eliminated. (Let us stress that widespread application of these devices, despite their high accuracy, is hindered by the high operating cost. Therefore, they are used with access from terminals to information carrying the highest security classification.)

And finally, the last procedure is physical connection. It is implemented by using keys and code cards. The keys are used to open standard mechanical locks on the terminals. The code cards are used for electromagentic locks. Authenticity is established by insertion of a code card in a special opening in the terminal. A special apparatus reads "magnetic data" from it and compares it to that stored in the computer system. When a match occurs, the terminal is connected. In a number of cases, the code cards contain not data, but light and dark strips, or they can be perforated, etc. Authenticity is established also by comparison with information fetched from the computer.

Practice indicates that code cards are more reliable than keys since it is technically more simple to make a copy of a key. The main drawback here is the possible loss of keys and cards and forgetting them in terminals. Therefore, the room where the terminal is located is secured. To leave, one has to open the door with the same card (key) used to switch on the terminal.

In addition to establishing user authenticity in computer systems, devices must be identified. This is due to the following reasons. First, several users with different rights for data processing may be connected to one terminal. But when data is output, it has to be sent to the user with the appropriate clearance. Second, some messages are to be output only to certain terminals. And third, in computer systems with a large number of communication lines, the probability of communication errors increases. Therefore, identifying devices assumes special importance. A user sending data to a computer system must be certain that it will end up only at the terminal with the address (identifier) specified. The same confidence is required with respect to the computer, the source of the output data (processing results).

Hardware facilities, code generators, and protection system programs are used for identification. A code generator generates pulses that interrogate, say, a terminal. Each terminal has its own code combination guaranteeing it unique identification.

Programs for establishing authenticity send the terminal password to the protection system, disconnect it when verification fails, and connect devices for issuing alarms. A computer's special identification is one of the simplest program methods in execution. It cannot be repeated by programs that are not part of the computer software. For example, in response to interrogation to establish authenticity, a computer can print out alphabetic characters in a sequence that cannot be repeated by unauthorized user programs.

Also used in identification are the cryptographic methods and similar translation functions discussed earlier. But here, the authenticity of a computer system device, not a user, is being established. Thus, the computer performs the actions to transform a password that coincide with the user operations. In the specialized literature, this mode has come to be called the "handshaking mode."

Device identification must be supplemented by I/O channel identification. Protection system hardware is used for this: registers and logic circuits, I/O channel checking circuit, register for checking channel secrecy level; character count register, etc.

The circuit for checking the data I/O channel checks the number of the channel through which the information is output from the computer. Determined thereby is any unauthorized change in direction of the data transmission through channels.

Data is input/output through specially dedicated channels as a function of the data security classification. In other words, a channel is authorized for transmission when its classification level is higher or equal to that of the data. The checking register interrogates and the value received is compared to the data classification. If the classification is higher, the channel is blocked. Let us stress that as a rule, channel identification is checked twice for "top secret" information.

The character count register is used to ensure complete transmission of information and to prevent false insertions in the text of a message going from a terminal to a computer and vice versa. Prior to the start of channel operation, the register is loaded with the number of characters to be sent. The register value of zero is the signal for terminating channel operation.

Let us turn to practical problems of maintaining security and integrity of data I/O. The major ones are: ensuring secrecy of the query and security of the output data, protecting processing results, and monitoring the interaction of terminal devices with the computer system.

Keeping a query secret requires, on the one hand, not allowing attempts at finding out the content of the query, and on the other, keeping secret (based on the security classification) the results of processing. Information on the nature of the query and about who is making it is secret. After comparing this data, a person intent on doing harm could draw a conclusion, for example, on the professional training and range of official duties and authority of the authorized user.

Secrets are protected by using organizational measures, primarily: enclosing peripherals, shielding against electromagnetic radiation, monitor checking of the operation of terminals, and introduction of a badge system. Also, it is necessary to ensure reversal of the password to the user after entering a call to the computer system.

The system of measures for protecting processing results includes safeguarding information output on printers, perforated media and terminals. A user must present evidence confirming his right to obtain it. Considered reliable evidence is a duplicate copy of the working list of the job sent to the computer for processing.

It contains the signature of the user certifying his right of access to the results.

To enhance the level of reliability, results (on media, print outs, etc.) are kept in special storage locations. The keys to them are kept by those responsible for protection.

The most effective way of checking on the interaction of terminals (users) with a computer system is the log. It may be kept manually or by machine. In the manual method, each user logs his name, terminal identifier, start/stop time of operation with the computer system and other information needed for comprehensive monitoring of access.

In machine logging, the protection system log maintenance program records in the log of revisions, as a rule, the full text of input information, terminal identifier, user password, type of changes made, addresses of data changed, and the data values before and after the change.

Let us stress that logging unconditionally of all accesses is not expedient. But there are situations calling for mandatory logging, for example, parallel access (updating) to one record by several programs.

The results of logging are the prerequisite for improving the protection system. Analysis of them forms the basis for developing new measures to prrvent unauthorized access to elements in the computer system, refining the rights granted to users and terminals, and recovering data when security and integrity is violated.

In practice, logging is performed as follows. Special terminals are dedicated to security, or ordinary terminals are time shared; information on occurring attempts to violate protection are output to them. Also, programs for checking access to information are built into the protection system. Thus, a user cannot bypass verification and obtain the right to unauthorized access.

Protection of Processing. The problem of organizing protection of information processing is complex and has many aspects. The limitations on solving it are the collective access of users to data bases in the computer system, conversion of information in virtual processors, the multilink structure of programs for data substantive processing and management, advanced methods for presenting (organizing) information on storage media, and the multimode operation of computers.

Protection has evolved gradually from the use of simple methods, means and measures to the implementation of the complex, say, dynamically variable models interacting with protected subsystems of data. However, maintenance of security and integrity has always been built on the base of software, hardware and organizational methods, i.e. there were no cryptographic methods.

Of necessity, developers have had to proceed based on the following:
--organization of checking of user rights to access protected elements (primarily programs and data during the computational process);
--maintenance of the correct, controllable and failure-free conversion of information in the processor under the conditions of multiaccess to the computer system;

--and development of sanctioned processing of information.

In addition to these basic measures, the security and integrity of the computing process has to be checked.

After authenticity of access is established, the user's right to access protected elements is checked. The need for checking is due to the following. Concentrated in a computer system are data files differing in security classification. In turn, each file consists of records, elements, etc. differing in importance. Files are processed by using operations: delete, read, write and others. Programs accessing data are input from different devices. All this compels restricting user rights to access information.

In the general case, user and terminal clearances are established. Clearances are also oriented to data bases, files, records and other structural elements of information. For any unit of information, there are specific actions that can be performed on it. Right to access is determined based on specific conditions: dependence on events, dependence on the action, unconditional access and others. Most advanced checking is implemented by a combination of conditions.

Establishing clearances (checking of rights) is enabled by using codewords, clearance profiles, protection lock mechanisms and protection keys. A codeword consists of several binary bits. Their number is determined, for example, by the number of records in a file to which access by specific users has to be restricted. The protection system analyzes the codeword after establishing user authenticity. For this purpose, a request for information (codeword from the user rights table) is compared to the codeword for the data classification. A match is considered authorization to continue the normal process of operation.

This approach is simple in implementation but rather ineffective. It does not take into account terminal clearances, the nature of the processing operations, and the features of interaction of several users. The effectiveness of this method is enhanced if there is provided in it a specification of the actions executable on the protected information, logging of access attempts and safeguarding of the protection mechanism proper. As a result, we will obtain the organization of data protection adopted, for example, in the IBM 360 operating system.

Operating system users are given the opportunity of requesting data protection by password when the data is stored (created), for example, on magnetic tape. This protection is implemented in parallel with the standard means of protection: data (file) set lables. A data set becomes accessible only when the user specifies his identifier.

Data sets on magnetic tape are equipped with a special catalog. An element in the catalog (one per set) includes a 44-byte set name field and an 8-byte password field. There is also a 2-byte counter that records successful accesses to the data set and a byte specifying the operations authorized on the set.

The flexibility of this approach lies in the capability of additional protection of the set of passwords. They are kept separate from user application programs under control of the operating system and protected by the main password. And the main password is an element in the set of passwords.

Developing clearance profiles means essentially gathering all the information determining the details of access to elements in a computer system. Clearance profiles are implemented in the form of a special table: a matrix for providing security (matrix for establishing clearances).

The first practical implementations of protection by using a matrix for establishing clearances emerged about 10 years ago. Since then, the method has undergone continual improvement, especially by using facilities to optimize location of the matrix in main storage. Thus, in the R system, a user is restricted in accordance with the columns and rows of the matrix, as well as when requesting statistical results of processing. In the KIKS system, a check is effected in accordance with a table that includes terminal operator names and codes (cyphers) corresponding to them.

Further, there are the mechanisms of protection (secrecy) keys and protection locks. As a rule, they are used to check the rights of programs to access protected objects. A lock is an element of data (constant), value of a variable, and program procedure. A key is a value specified by a literal (constant), identifier of a variable, and name of a procedure.

Based on user requirements, protection keys and locks are assigned to various structural units of information (file, record, element, etc.). For each unit, a lock(s) is related to a specific action or function that has to be performed on this unit of information. Thus, in some systems, there are locks at three levels of access protection: access to information in the entire system, to information of subscribers (enterprises, building, etc.) and to specific data.

The most flexible and constructive solutions for organization and operation of the protection mechanism are those provided in the CODASYL approach. It can be said that it is universal and convenient for application in the majority of computer systems.

In this approach, protection locks are specified at the levels of the scheme, range, record, element of data, group of data, set and records of the set members.

For each level, one can specify several locks, relating them to a specific instruction in the instruction language (data manipulation function). Moreover, there are locks on the descriptions of the location of data in main storage and on the locks themselves.

Changes in user requirements for protecting their information do not affect the representation proper of it in the computer system. Protection effectiveness is also enhanced when those responsible for protection, in specifying locks in the general definition, safeguard them from changes from the direction of user programs. In other words, protection in the scheme has priority over subscheme facilities.

Keys are distributed among users by those responsible for protection or administrators. They must uniquely correspond to the locks, i.e. be assigned to units of information at one common level.

Let us explain the difference between keys and passwords. The concept of a "password" is considerably simpler since a password may be the entry to a procedure for generating a protection key. Also, a system administrator does not have the right to assign a protection key (but he may for a password). Keys and locks are compared by facilities of either an applications program, data base management system or operating system. In practice, these facilities are not encountered in "pure" form. In checking, a key is compared to a protection lock. To open a lock, represented in the form of procedure, it is necessary to perform computations on the key in accordance with an algorithm specified by those responsible for protection and defined in the scheme and (or) subscheme. As a function of the computation results, a decision is made to authorize access (processing) or the process is halted, an alarm signal is generated, the terminal is disconnected, program execution is halted, etc. If the value of a lock is a literal or lock name, it is opened when the values of the protection key and lock match.

The concept of keys and locks extends to the security not only of processing, but also of integrity. Thus, logic errors are prevented by stopping incorrect, uncoordinated, senseless operations on information, and coordination of interrelated data is confirmed.

Let us turn to a discussion of the second point: maintaining correct, controllable and failure-free conversion of information in the processor under the conditions of multiaccess to a computer system. The main task here is to have the capability of locking memory during operation of the computer system, i.e. of preventing unauthorized intervention of any program in the activity of other user programs and the operating system. Each program (process) must not distort other processes and be executed independently. A minimum of three modes of access to memory is required during execution: read only, read and write, and just execution of the program (i.e. just with the individual instructions included in it).

Let us explain the last mode. It is oriented to the region of memory in which the program is stored. Thus, during execution, the program is inaccessible for reading and (or) writing by other processes. This is especially important to protect, for example, the author's rights of the developers: if the program is made available for temporary use, it is not possible to copy it without permission.

Used to maintain a monitorable, controllable and failure-free process are protection register circuits, code words and memory paging, privacy bits, code redundancy, segmentation, etc. Their application differs in the level of effectiveness and in different functional capabilities. Base registers are the most durable and cheapest; memory paging is the most expensive. They have no fixed logic connection between them, i.e. they are developed independently. The means of implementing them also varies. On the other hand, there is a relationship between the basic forms of use of programs (data) and the organization of their protection.

Let us first discuss the processor protection most general in design. In the majority of third-generation computers, main storage is divided into fixed-length areas, as a rule, with 2048 bytes each. Each area is assigned a storage key. A program obtains the right to access only when there is a match between the storage key and the protection key stored in the program status word. Bit values in the storage key indicate the actions authorized with it: writing of information, fetching. Thus, a fetch protection bit value of "1" inhibits writing and fetching in this area of storage. A value of "0" enables fetching by all programs, but writing by only those with a bit combination in the program status word equal to the write protection bits in the storage key.

The purpose of the parity check circuit is to detect failures when data is moved within the computer. A check bit is put into each byte so that the bit sum is even. When data is transferred between machine devices, the check circuit checks the parity; if there is an error, the transfer is interrupted.

Of special interest to protection is the type of interruptions: program and interruptions for the check circuits. Program interruptions of CPU operation occur with the following errors: reference to a nonexistent storage address, occurrence of unusual situations (division by zero, storage overflow and others), and execution of an inhibited operation code. Check circuit interruptions ensure protection against malfunctions in equipment operation. An example of such a circuit is the parity check circuit.

And finally, code redundancy is a development of the capabilities of detecting and correcting errors. By using redundant bits, codes are formed that enable, for example, detecting dropped bits.

Protection register circuits are used extensively in computer systems. They are especially effective when a computer operates in the multiprogram and time sharing modes. This requires some explanation. There are two ways to design data protection in main storage during processing. The first is the development of the list scheme. The access check is made from the list, i.e. the program has to present its identifier/name. It is checked against the list kept in computer storage. Access is possible only when the program name matches one on the list. Thus, with each reference, the access check has to be repeated. In the second case, the right to access data (programs) is granted by presentation of certification. The protection system responds to the certifications that are selected by the user himself (in the general case, there may be several of them) to obtain access to the required set of data.

Let us discuss the first direction. An elementary protection register circuit is described as follows. Added to the processor is a special double register (descriptor, base-limit) with two parameters: base and limit. They define the limits of storage that can be accessed by a program. To implement this approach, a privileged mode is required when the descriptor register proper is processed: values of data to be stored and right of the program to access are checked--otherwise protection becomes ineffective. Introduced for this purpose into the circuit is a flip-flop for the mode (indicator, task-supervisor bit). It takes one of the two values, "zero" or "one." The value "one" indicates the privileged mode, i.e. one of the operating system programs functions: the supervisor which is given the right of loading the descriptor register with a new descriptor.

Protection is effected the following way. The address specified in the instruction counter is checked to see if it is within the storage area bounded by the base and limit. If not, an abnormal situation results. If this situation does not arise, the addresses contained in the instruction are similarly checked. A successful result from checking enables execution of the instruction. Otherwise, an abnormal situation occurs and the task-supervisor bit is set to one, keeping this value until the causes of the abnormal situation are cleared up.

Improving the protection register circuit has compelled an increase in the number of base-limit registers. In doing so, the versions that are emerging call for assigning to the same register the functions of checking the instruction address and of the instruction counter. Other descriptor registers are used for correctness of addressing of operands (one for each data set--segment, file). In this case, the segment number is the argument for selecting a register, i.e. the number is part of the address.

Bits, as a rule, two, are being added to the base-limit register. Their function is to qualify the operations (instructions) executable on a file. Combinations of bits indicate allowable and prohibted instructions on corresponding segments.

Development of the second direction started in the sixties. In principle, the hardware facilities described earlier are suitable in this case. However, high effectiveness can be achieved by using special machine instructions (operations) that allow direct hardware processing of certifications. They (the certifications) contain the name of the segment and the indicator of access to it. Descriptor registers are called certification registers. Special instructions are used for manipulations with them. They are set apart into a separate group and enabled (inhibited) separately from other instructions.

Let us explain the principle of organizing memory protection during processing by using the certifications in the example of the project at the Computer Research Institute at the University of Chicago. Introduced into the processor are enabling flip-flops that, in turn, are divided into two groups. The flip-flops in the first group are set to a certain state based on the value of the bits in the certification register associated with the operand; and the second, in accordance with the values of bits in the certification register associated with the instruction counter. The task-supervisor bit is eliminated from the processor, i.e. there is no privileged mode.

The file access indicator may assume one of the following values: read data, read and write data, read certification, read and write certification, just execute program, I/O and input.

Segments differ: one contains information, the others just certifications. Thus, either information or certification can be fetched from storage, and as a result, a program is limited in its actions to only those actions stipulated in its certifications.

Access to a segment (certification or data) is possible only after its certifications have been recorded in one of the certification registers. As a result, there is complete determination of the actions executable on the data or certifications (reading of certification, just execution of a program, etc.).

Let us explain the purpose of the enabling flip-flops in which certifications for I/O and input are recorded. Certification for "input/output" enables functioning of a program segment having an input or output instruction. Certification for "input" realizes a call of a program for another. In doing so, the call occurs during loading of certification of the called program by a special instruction into the register of certifications for "input."

This approach has evolved into designing pseudocertifications. They are needed to protect information kept on storage media (on external storage). For each file placed in external storage and having a pseudocertification, there is formed a real, actual certification. The set of certifications pertaining to one user's information files is his file catalog. As a result, the effectiveness of the protection system is enhanced based on the files being unequivocally affiliated with a specific user.

Let us compare the directions discussed. Use of the list system is more tedious. Checking each reference entails searching the list of subjects (programs, tasks, processes) given the right of accessing information. Used in the mandate scheme is a simple comparison and there is no need for scanning a list of subjects. But other complexities arise. There is a need of monitoring the transfer of powers among subjects and establishing authenticity of accesses.

The highest effectiveness is achieved by a combination of the directions. User interaction with the computer system is built in two stages. For example, by entering a password from a terminal (first stage), the user receives a pseudorandom number (second stage). Transformation and correlation of it produces the capability of obtaining the right to interact with the computer system.

Successful organization of authorized processing of information in a computer system requires: joint protected use of programs and data, efficient distribution of resources servicing processing, a controllable and flexible scheme for transferring among users authority to access files of information and programs.

The need for joint use by programs of common data occurs under the conditions of multiaccess to a computer system. If programs are isolated into parts for processing identical information files, main storage will be wasted unjustifiably and the process of making changes to interrelated data complicated. Consequently, protecting information integrity will be violated.

But joint use of data (programs) requires additional protective measures. First of all, the programs interacting with jointly used data must be independent and isolated from each other. There has to be a mechanism for switching control between programs and supporting access to common data. And finally, attempts at uncontrolled changes and processing of joint data must be blocked.

Under conditions of joint use of data, mutual isolation of programs is achieved by introducing a descriptor register into the processor, which points to a common segment of information. A program is "prompted" as to which storage area it has to access by using a register specification: its number is indicated in one of the bits in a program instruction or a special field with this number is inserted into the instruction.

This mechanism illustrates the principle of mutual isolation of programs that process common data. To exchange information with each other, they call the supervisor; it, in turn, controls the process of data transfer. Protection reliability is achieved because the programs cannot change the contents of the descriptor registers.

Under real conditions, situations arise when it is necessary to protect the processing proper of common data of resources, i.e. to realize the integrity of parallel processing. Problems of parallel processing are inherent also to the software, hardware and other components of a computer system. Here is an example.

The most typical situation, called "blocking" ("deadlock") in the specialized literature, is the direct dependence of one resource on another. Assume there are two programs, each of which must process file A and file B. The first program has to process file A first, then file B. The other program performs these operations in reverse sequence. Hence, after obtaining access to file A, the first program will be waiting until the second releases file B. A similar situation occurs with the second program. This is how blocking occurs.

In the next example, permitting uncontrolled parallel access will "wipe out" executed operations. Let us assume a program has updated some element in a record. It, however, will be interacting with an "old record" if another program obtains access to the updated element, having the capability of changing it prior to the completion of processing by the first program.

Protecting parallel processing is governed by both the degree of overlap of operations and the actions that have been requested with respect to a resource in the computer system. Programs for creating, updating (writing) and querying (reading) theoretically can have a different degree of overlap (concurrency). But the program for creation must be completed before the others and, as a rule, cannot be overlapped with them. In turn, parallel execution of update and query programs is allowed.

Specific design solutions in implementing concurrency depend on the features of the operating situation: the types and systems for managing data bases and the computer operating systems. Thus, in the YaP/1 system built by the firm RKA, there is no parallel access; and in Western Electric's SU-1 system, a program cannot open a file when it has already been opened for modification by another program. Thus, during any changes to a resource, exclusive use of it has to be declared; and conversely, if a resource is not being modified (say, only reading of a file occurs), joint processing is permitted.

Inhibiting joint use means sequential processing of the resource, i.e. as it is released, it is transferred to the competing programs.

Computer system software has flexible and reliable facilities for controlling exclusive and joint access by users. The desired form of resource control, exclusive or joint, is indicated in a computer operating system special macroinstruction, "Place in Queue," based on requested actions. Exclusive control must be requested for additions, corrections, modifications and other actions that change the resource. Joint control supports only the mode of reading information without any changes to it. Let us note that access to information protected by joint control is closed to programs requiring exclusive control. Also, all exclusive requests are mutually protected.

Parallel processing requires adhering to a number of rules for protection (otherwise, information integrity is violated--deadlocks occur). The requested resource must be free, i.e. ready to operate with the new reference coming to it. It is advisable to release it as early as possible; this enhances the efficiency of computer system operation and speeds up processing.

Whenever possible, exclusive control of information should not be specified, especially in cases not requiring change, modification and correction of information. But it is desireable to request at the same time all resources needed for the user (program). It is clear that blocking is prevented since processing will be completed before the other users will be able to obtain access to control resources.

And finally, when a deadlock occurs, integrity is recovered, as a rule, by excluding the program that caused minimal changes or was started in the last queue.

Another important question in organizing sanctioned processing is providing for joint ownership of programs and data, as well as protecting transfer of authority for possession. Let us single out two forms of ownership: isolated and collective. Isolated does not provide for exchange of authority on controlling programs and data. Users are autonomous; each interacts with his own information files. But with collective ownership, powers may be spread among users. In other words, the users subscribe, lease and "hire" someone else's programs and data.

Based on specific conditions (operating environment, features of queries to computer system, etc.), methods of transferring authority vary. In the general case, authority can be transferred by: compiling a list of the names (identifiers) of users who have obtained the right (permission) for access or issuing one-time permits to individual users. A list is produced by those responsible for security and it is coordinated with the owners of the information files and programs. Use of a list is preferred when a group of dependent users works with the information, for instance in solving a common problem.

In the transfer of authority, the protection system must monitor the authorization of the user that received it. Not every user can impart the right of possession of programs and data or perform various actions on them. Here it is especially important that the protection system restricts the user's right to handle even his own data (programs). In certain cases, barring the transfer of authority is the only capability of preventing misappropriation of information. For example, in forming a matrix of security for a group of users working on a common problem, a manager sets the conditions for noninclusion in the matrix of project workers from another group.

Thus, a dual hierarchical protection of data processing is organized. And the restrictions introduced by the protection system must have a higher priority than the permissions granted by owners of information and programs.

Another reason for restricting the transfer of rights to possession is the risk of destruction of programs and data by the user borrowing someone else's programs. Also, after obtaining access to information for one purpose, he can illegally read it and send it to his "boss." Such programs have come to be called "trojan horses" in the literature: in addition to the duties entrusted to them (implementable functions), they also illegally copy and send the information to their "bosses." Thus, it is necessary to ensure protection of both the collective ownership and the transfer of rights. This can be done by safeguarding leased programs, by designing protective subsystems and by cataloging files.

Safeguarding or fencing is the operation of a leased program in a specially allocated partition of main storage. In this partition, the program has access to processing information, but cannot sanction its transfer to another memory partition. And transfer of information being processed and results obtained is also inhibited.

Safeguarding provides for the different modes of operation of a leased program. While making his data available for processing, the user suppresses (permits) the mode of changing it, i.e. only reading without writing is allowed or vice versa. In doing so, protection is sharply complicated.

Protection becomes especially complex during access at the same time of several programs in different modes, for example, by one authorized to read only, and by another allowed to write information again and again. In this case, control of safeguarding must be strengthened for a program writing data may become a "middleman" between the program "reading only" and the information in main storage. It writes information to the same memory location accessible to the "reading" program. In other words, a user changes the mode of access of another without authorization.

For protection, it is necessary to establish and fix the unambiguous correspondence between a program and the memory partitions into which it is allowed to write data. And the partitions must be made inaccessible to the "reading" program.

Safeguarding, however, does not protect data against destruction by programs that are leased and "ill-intentioned" programs that attack the data of a user in main storage. "Ill-intentioned" programs, for example, scan memory and look for secret data, destroy the synchronization of file processing and create other threats to security and integrity.

By definition, a protected subsystem is a set of programs and data placed in a memory location that is sealed off against access by other programs. The location is surrounded, as it were, by an "impenetrable barrier" blocking outside access to the programs and data contained in it. Access is granted only to the programs included in the protection subsystem; and they are fully responsible for protecting the data.

Let us stress that the user is given the capability of setting up any method of checking access to information in a protected subsystem. This check is made by special programs that are part of this subsystem. They support communication with the "outside world" and record accesses. Thus, access to information is possible only by calling the programs, which, in turn, are protected themselves.

Yet another advantage of the protection subsystem is the capability of a differentiated approach to exchange between it and users. Users have the right to call the protected subsystem only through their own programs, each of which has been authorized particular actions, for example, unlimited access to all information, reading part of the data, etc.

In the general case, several protected subsystems can be placed in main storage. In this case, integrity and security is maintained for both user programs and the computer operating system since it (the supervisor) is closed to access on the part of user programs.

File catalogs are oriented to users associated in the process of working on one problem into collectives. Each collective has its own catalog with the capability of organizing differentiated user access to the information common to them. There is communication between catalogs that enables exchanging rights to possession.

Let us examine the features of protecting the transfer of rights to possession based on the approach adopted in the Cambridge system. Its advantages include: full coordination and controlability of user access to all information in the system and to individual facts, wide range of privileges and prohibitions imposed on possession of files, and flexibility in making changes to rights granted earlier.

In the Cambridge system, a catalog has two levels. In the top (system) level, there are references to user catalogs. Kept in user catalogs are references to user files and to supplementary and mandatory information. Mandatory information includes the file name, rules for access to it and other items. Supplementary information, for example, includes the date of the last access to the file.

Upon creation, each file is assigned a name consisting of three parts. The first part of the name identifies the owner; the second and third parts are arbitrary (prescribed at owner's option).

To protect rights to be transferred, a fourth part, file status, is used. The characters in the status word define the actions the file owner allows (prohibits) to co-owners for use of it. In addition to the owner, the Cambridge system allows for co-owners, partners and key holders. Partners are specified in a special list. As a rule, the list identifies the programmers working in a group on a common task. A key holder knows the key that he must enter (key in) while requesting access to a file.

Different rights are granted owners (co-owners) as a function of their status. In the general case, the following actions with a file are allowed: change status or read, implement free access, only load for program execution, only read, delete, change status or read, and prohibit access.

Authorizations are transferred and access is checked by using a system of orders. An order is a permit to process information when certain conditions are observed. For example, a partner with the last name of White receives free access to the files owned by Black if he enters the keyword "Union" at the terminal. Another example of an order: the files of the same user can be accessed with the right of "read only" by all users in any case.

But while permitting the performance of actions on his own files as a whole, their owner can vary the access to an individual file. A 20-bit word is associated with each file. It is divided into four groups. The bits in the groups indicate the rights pertaining to the actions performable on the files granted, respectively, to the owner, partners, key holders and others. When accessing files, a user program presents a request word with information on actions required. As a result of a special check of the file, order check, access is authorized (prohibited).

Partners, after obtaining free access, automatically become owners, i.e. they have the right to transfer rights. In the process, new file orders are formed or old ones are destroyed. Orders are generated (destroyed) by special instructions.

Let us turn to the method of protecting information integrity in the Cambridge system. A special character is inserted in the file status. It instructs the system to copy data from disk to tape. Copying is performed regularly (at least once every half-hour) after a file is generated. Thus, if information is wiped out, the capability for recovering it exists.

Protection of Transmission and Storage. To protect information during transmission and storage, organizational measures and cryptographic methods are used. The technological feature of the stage determines the specifics of the organizational measures and protective transformations corresponding to it. Thus, information is kept in a computer system for a long time, but sent over communication channels at a high rate; during storage of a file, it is necessary to ensure the independence of its records, i.e. each of them must be processed separately from the rest; the percentage of errors during transmission is higher than during storage; when data is transmitted, it has to be decoded at all receiving points, but when stored, only in one location; changing the conditions of operation of devices for storing and transmitting information affects its integrity in different ways.

Cryptographic methods prevent the use of information intercepted from communication channels or stolen since in encrypted form it is of no value to the malefactors. Protected transformations are essentially the only way to secure information transmitted over wideband communication lines, the telegraph, the telephone, etc., beyond the limits of the computer center. Safeguarding communication lines over their entire extent sharply increases the cost of the information sent.

Organizational measures supplement protection of information at the stages of storing and sending it. They also ensure "support" of the cryptographic methods, for example, securing the storage of encryption keys, closing off access to units for encryption and communication equipment, etc.

Encryption is the transformation of a series of characters in the source alphabet into a series of characters in the same or different alphabet. The transformation is performed according to a particular algorithm by using an encryption key. Decoding, obviously, is the reverse process.

Various classes of encryption are used in computer systems. Protection transformations are also implemented by various methods. To show the interrealtionship between methods of implementation and classes of encryption, let us discuss protection transformations in computer systems.

The simplest and most well known is the method of substituting a character in a different alphabet for a character in the source alphabet. And the substitution may be accompanied by a shift by a certain number of letters in the new alphabet. But this cipher is precarious and unreliable. Based on the frequency that particular letters occur in a language, the information can easily be decoded by using cryptanalytic methods.

The method is improved by using several alphabets. Each letter in the source text (alphabet) is encoded by a corresponding letter of another alphabet. Assume that coding the expression "vychislitel'naya sistema" [computer system] is required. Including the blank space, it contains 20 characters. For encryption, let us use 20 alphabets, each containing 33 Russian letters and one blank character. Let us number the letters in each source alphabet as follows: 0 = blank space, 1 = A, 2 = B, ..., 33 = Ya. As the key, let us take one arbitrary letter from each alphabet for encryption: N Sh O space " F YË " YË S Zh Shch T A O S YË A P P. It is easy to see that the encryption key is just a random set of letters with no meaning of its own.

To encrypt the text, we have to add to the number of the position of each letter in the source alphabet the number of the position of the corresponding letter in the key. If the sum obtained is greater than 34 (the number of letters in one alphabet including a blank space), we subtract 34 from the sum. The result obtained will also be the true value of the letter in the encrypted text:

V	Y	Ch	I	S	L	I	T	E	L	'	N	Y	Y	space	Ts	E	N	T	R
3	29	30	10	19	13	10	20	6	13	28	17	29	11	0	24	6	15	20	18
N	Sh	O	sp	"	F	YË	"	YË	S	Zh	Shch	T	A	O	S	YË	A	P	P
15	26	16	0	30	22	7	30	7	19	8	17	20	1	16	19	7	1	17	17
R	U	K	I	N	A	P	O	L	Yu	B	I	N	K	O	Z	L	O	V	A

[as published]

Thus, from the source text "vychislitel'nyy tsentr" [computer center], we obtain the meaningless combination of letters" "rukinapolyubinkozlova". Let us note that the security of the cipher is enhanced by increasing the number of alphabets used in encryption.

Enhancing resistance does not conclusively resolve the problem of frequency analysis, i.e. the characteristics of occurrence of letters inherent to a natural or algorithmic language remain. The characteristics are smoothed by using monophonic ciphers (they smooth the occurrence of the individual letters (characters) in an alphabet).

Let us consider an example (for better comprehension, examples are given in the Russian language). Assume the text "tsifrovaya EVM" [digital computer] has to be encoded. Let us take into account that the letters, say, Ts, E, F, etc., occur in the Russian language considerably less often than A, I, S, etc. Let each letter in the source text correspond to a combination of one, two or three letters of a monophonic cipher:

Source text:	Ts	I	F	R	O	V	A	Ya	space	E	V	M
Cipher:	chor	iu	s	ak	y	u	il	d	r	ub	okn	ye

Another method of protection transformations is transposition. It is implemented by various methods. One can transpose characters (letters) in a source text, for example, by writing the source text in rows of a matrix, and reading it for encryption purposes in the columns. Another method is to divide the source text into groups of an identical number of letters (four to six on the average). Then the positions of the letters in all groups are interchanged.

Cryptographic protection by using transposition is very effective. But it should be combined with other methods. Let us turn to the preceding example. Let us break up the derived encoded text, "ChORIUSAKYULDRUBOKNYe" into five groups of four letters in each: ChORI USAK YUIL DRUB OKNYe. [as published] In each group, let us transpose the positions of the first and the fourth, as well as the second and the third letters. The result of applying the function of transposition is:

IROCh KASU LITsY BURD YeNKO. [as published]

Let us stress that successive encoding of information by several methods in addition to enhancing resistance allows a paradoxical reaction: "weakening" of the protection transformations, since the information enciphered "in one direction" by one method can be decoded in the "opposite direction" by another.

The protection transformations discussed above cannot be considered reliable and effective. Improvement in the hardware and software for encoding information is opening new capabilities for implementing methods of protection transformations. But in the process, new demands are imposed on encoding as well: minimal information redundancy (small increase in the amount of the encrypted information compared to the source text), low susceptibility to encoding (decoding) errors, invariance to intramachine and intrachannel representation of data in a computer, rapid encoding (decoding), and resistance to attempts of unauthorized decoding.

Realizing protection transformations with regard to the new requirements in computer systems is done by software or hardware. The basic methods here are analytic (algebraic) transformations and the gamut. Analytic transformations encrypt text broken up into fixed-length blocks. The key is a matrix by which the vector-block of plain text is multiplied. Assume for example that the digits 1, 6 and 9 are to be encrypted while the elements in the matrix key are 2, 4, 6, 1, 6, 7, 9, 8 and 0. Then the encrypted text is obtained by multiplying the matrix rows by the vector of plain text:

$$\begin{pmatrix}2&4&6\\1&6&7\\9&8&0\end{pmatrix} \text{X} \begin{pmatrix}1\\6\\9\end{pmatrix} = \begin{Bmatrix}2\text{x}1+4\text{x}6+6\text{x}9\\1\text{x}6+6\text{x}6+7\text{x}9\\9\text{x}1+8\text{x}6+0\text{x}9\end{Bmatrix} = \begin{matrix}78\\105\\57\end{matrix} \quad \text{[as published]}$$

Let us note that algebraic transformations are tedious and entail considerable outlays for machine time and computer storage. Modified versions of algebraic transformations have been developed to reduce encryption time and the size of main storage taken up by the matrix key.

In recent years, maximum efforts of designers-cryptanalysts have been directed to research in the area of software and hardware implementation of the gamut method. A gamut is a random sequence of numbers, ones and zeros as a rule, formed by using a pseudorandom number generator. The generator built by software is a formula in which the source number is substituted; the result of transformation of the number becomes the source number for deriving the next pseudorandom number, etc. Assume the first and fourth digits in the source number 1952 are to be cubed and the results added to the source number. Repeating the process, we obtain a sequence (series) of pseudorandom numbers: 1952, 1961, 1963, etc. Continuing the process, however, leads to confluence of the series, i.e. starting with some iteration, the numbers in the series will be repeated.

Therefore, it is advisable to develop a pseudorandom number generator that ensures their repetition period allowable for the purpose of encryption. An "infinite" series of pseudorandom numbers (gamut) is built; from it, the encryption keys for information to be sent and stored are selected. Each word (character, number) in the source text gets its own unique key. By using the logic operation "exclusive OR" digits in the source text are combined with the encryption key (gamut). The "exclusive OR" logic operation is reversible, i.e. it can decode text by adding the key value to it. For example, the source text in binary notation is 1001101, the encryption key is 0111010 and the result of encryption is 1110111. After adding the results to the encryption key by using the "exclsuive OR" logic operation, we again derive the source text, 1001101.

The gamut method is strengthened by inserting intervals into the series of key characters. The characters are counted and some of them eliminated; for example, only every fourth character is used for encoding from the series 1001110101111000. Then the encoding key will be 1110.

A gamut is generated by the simplest hardware by using a shift register with linear feedbacks. It includes cascades, to which clock pulses are fed, the feedback bus, and switches supporting the shift function.

The output of the shift register with linear feedbacks is an encryption key in the form of a pseudorandom series of ones and zeros. Clock pulses are fed to the register input for this which then go though the feedback bus. As a function of the connections of the feedback at the output of the last cascade, the pseudorandom combination (gamut) of ones and zeros is generated.

Fed to the output of the last cascade is the plain source text, also represented in the form of ones and zeros. The gamut is superimposed on the source text: bit-by-bit application of the "exclusive OR" logic operation. The result of the gamut superimposition is the encrypted text; the text is decoded in the opposite procedure.

Sometimes two additional registers, one of which is a control, are introduced into the simplest scheme described. As a function of the value of the control register output, the output signal from one of two working registers is taken for encoding. The presence of the linear relationship between the source and encrypted text compels complicating the scheme. In other words, after intercepting only several bits of source information and the encrypted text, one can disclose the message. The linear relationship between the source and encrypted text can be eliminated completely by combining the two protection transformations of substitution and transposition. In this case, without knowing the key it is practically impossible to break the encrypted text.

In the hardware implementation of the substitution method, a combination of zeros and ones is fed to the inputs of the substitution unit. The unit intersperses source values and may also add zeros and ones to them. For a unit with three inputs, the source values are: 000, 001, 010, 011, 100, 101, 110 and 111; the output values corresponding to them may be, for example, 11, 101, 010, 000, 011, 010 and 110. Let us note that the engineering implementation of the unit is complicated and costly. Therefore, the number of its inputs, as a rule, is limited.

A transposition unit only shifts and displaces a signal, i.e. it does not perform nonlinear transformations. For example, a "one" is fed to input No. 29, but the switch circuit within the unit will shift it and send it to output No. 30. Such devices are inexpensive. But they must be protected by using organizational measures. Otherwise, an unauthorized user can break the switching scheme by feeding a signal to each input and recording its emergence at the output.

A device that combines several transposition and substitution units is used extensively in computer systems for encoding (decoding) data sent over communication channels. An example of the device is the LUCIFER coding equipment (its concept has been adopted in a number of countries as the standard in practical implementation of the methods of protection transformations).

LUCIFER is a general-purpose system interfaced to terminals. The system encoding equipment can operate in different modes: switched only for reception of information, i.e. for transmission of plain text and decoding of information received or it can encode data being sent and decode that being received. It is made up of a cyclic key register, source text registers, intermediate registers, switches, adders, and encrypted text registers. The source information in the form of ones and zeros goes to the transposition unit. In accordance with the switching scheme in the transposition unit, the signals are shifted and sent to the inputs to the substitution units. The substitution units are in state 0 or 1. The state of each unit is determined from the value taken from the 128-bit key register. The key register is loaded before starting encoding.

After passing through the substitution units, the information is supplemented with zeros and ones. Then it is fed to the input of the transposition unit, etc. As a result of several iterations, the encrypted information is generated at the output of the transposition unit.

This is the basic scheme of operation of the LUCIFER. There are, however, a number of refinements shaped by the specific implementation. The source information is loaded into two 64-bit registers, separated into 16 parts. Based on the value of a bit in the key register, the positions of the information in the adjacent parts may or may not be interchanged. The entire substitution unit cannot be switched to states 0 or 1, but each information bus in it can. The contents of the key register are shifted cyclically by one bit both at the point of encoding the information and at the point of receiving it. There are also other "features" of LUCIFER functioning.

To rpotect the security of information, it is important that the key itself not be sent over communication channels. On the other hand, synchronization of the processes of encoding and decoding is required. LUCIFER has a built-in password generator for this. It generates a password for each encoded block of source information. The source text is combined with the password and sent for encoding.

A like password is generated at the point of information decoding (they are synchronized by using pulses from binary clocks) and the correspondence between the information blocks sent is checked. The information is decoded at the reception point by adjusting the code key and password for each block of text sent.

Let us stress that any source word sent an infinite number of times will continually receive different encrypted equivalents. Thus, the level of protection of information security in a computer system is sharply enhanced. Also, the use in LUCIFER of error correcting codes (based on information redundancy) maintains the integrity of messages sent.

The classes of problems solved, the location of information processing points, the user requirements, etc., determine the feature of encoding equipment connection to a computer system. The main methods of connection are: "terminal-encoder-I/O control processor-interface-computer" (or "computer-encoder-modem-communication line-modem-encoder-computer").

Connecting coding equipment to a computer system requires, first, compatibility between the data transmission equipment and the coding equipment, and second, controlled exchange of keys between users at message sending and receiving points. Compatibility is achieved, as a rule, by encoding only the fields of data being sent, and service information, the message header for example, remains unchanged. As a result, the data transmission protocols in effect in the computer system are kept.

Key exchange is controlled by various methods. In one method, special centers for distribution of keys are organized in a computer system. The code keys for all users of the computer system are kept in them. Each user, in turn, is furnished with a key for accessing a particular center. Protection of access to information is thus afforded.

To organize communications between, say, two users, they must send access keys to the distribution centers. The encryption keys received from there are the basis for forming the final (resulting) encryption key. It is built by applying the "exclusive OR" logic operation to the encryption keys, i.e. their values are added. The resulting key can be broken only by knowing all its components.

The evolution of the mathematical theory of complexity of computations has facilitated formalizing the processes of exchange of keys. The capability has emerged of estimating the degree of risk that occurs when information is intercepted, the time and cost of decoding keys, etc. In the majority of methods that are evaluated in terms of computational complexity theory, the base concept of the "public key" is used. Let us consider one basic method of exchange based on this concept: the system of public distribution of the key. Users setting up communication with each other exchange protions of information. It is combined with thoroughly protected information kept at the user sites. The result of the combination is the code key. Let us note that intercepting the portions of information sent over communication lines will not help malefactors in computing the code key: it is very difficult to solve the equation linking the known values (intercepted portions of data) and the code key.

Let us turn to a consideration of organizational measures for protecting information transmission and storage. When sending data over communication lines, it is very important to protect them against the effect of electromagnetic fields, i.e. to uphold information integrity. Special screening protective insulations are being developed for cables. Their effectiveness is determined by the features of the insulation. The highest quality of protecting against electromagnetic radiation is achieved by insulation organized as follows. The protected "wire" is placed in an aluminum sheath, a steel corrugated sheath and a polyethylene tube. Insulation capabilities are enhanced by adding lead sheathing to it and replacing the polyethylene tube by jute braiding.

In addition to protecting the "wires," communication line apparatus has to be protected against high voltage penetration. The most effective is the cascade scheme of protection. It is formed of: diodes placed before amplifiers at input and output, low-voltage suppressors connected between wires in the secondary circuit of the line transformer, and high-voltage gas-filled suppressors installed from the direction of the communication line.

Switching radio relay lines to lines with less radiating energy such as coaxial and fiber-optical promotes protection of data security during data transmission.

Designing organization measures for information storage protection is largely determined by the type of information media, limits on time and cost of protection, features of computer center functioning, etc. In computer centers where magnetic tapes make up most of the media, the organizational measures are directed to protecting them during storage. The information on them must periodically be copied from one medium to another. The period for recopying is determined by instructions for storage (as a rule, not less than once every several months). When the data is being copied, the check sum has to be computed. This helps detect errors that arise during storage.

Library location must meet the specific climatic conditions, i.e. the temperature and humidity have to be kept within prescribed bounds. This is especially important for perforated cards and tapes. Magnetic media shoul be placed on specially equipped racks, and software is stored separately from data. Media containg programs must not be taken outside the computer center (except copies). They are placed in plastic bags (cartridges); those containing information with a security classification are also kept in locked boxes (safes). Access to the library is restricted. A library custodian should be appointed. His duties include: keeping track of media issued, recording requests for issue, maintaining information security, etc.

Magnetic disks are not strong mechanically; for example, if the magnetic heads touch the disk surface, it heats up and distorts the data on it. In the literature, this phenomenon is called "scoring." When magnetic tapes are dropped, the data on them are not always destroyed; but on disks, the risk of distortion is considerably higher. In this connection, before processing, it is wise to check a "suspicious" disk surface to detect possible destruction.

Computer center functioning features have a considerable impact on keeping information during storage. Let us mention here two alternatives: making copies of all information media or organizing circulation of information on media. The first is reliable but requires considerable expense for acquiring and storing media. In the second, a group of media is allocated for information circulation based on conditions specified by users. The number of media, as a rule, is three to five.

A file of information used in processing is assigned the number 0, the new file is +1, and the preceding versions are -1, -2, -3, etc. Circulation (rewriting) occurs after completion of processing, running a job, or at the end of the work day. Files are transferred on magnetic media so that the file with number +1 is written over the file with the highest negative number.

Thus, integrity protection is assured since destruction of any version (generation) within the bounds of those on hand allows recovering it. The previous generation is used for this purpose and the required data read.

What Has Been Done So Far. The aim of this section is to acquaint readers with practical developments in organizing specific protection systems abroad. An attempt has been made to cover the most interesting design solutions, especially for recovering destroyed information. A more detailed and expanded description of specific protection systems is available in the literature (see the bibliography at the end).

In IBM's automated system of administrative management, data is protected by hardware and software methods. Hardware facilities enable page partitioning of memory, checking for parity, privileged instructions, interrupt schemes and others. Depending on the computer model, a user password is suppressed or printed during access. Thus, the user password is suppressed on the IBM 360/65, but printed on the IBM 360/40.

The OS/360 operating system offers the capability of identifying users by using a 3-6-bit alphanumeric code. It is entered into the computer prior to the user's request for service and changes when its time expires.

User rights for execution of operations are recorded in tables which can be accessed only by operating system programs. The tables are kept in a special memory partition with restricted access.

If a user forgets to disconnect a terminal after completing work, this is done automatically by special programs (after referencing a timer).

Another IBM product is the ADEPT automated data processing system. It is used for information acquisition, processing and storage at various institutions. The IBM 360/50 computer is used in ADEPT and thus the protection hardware facilities are common to computers in this family. Also provided is a data reading check scheme protected against unauthorized execution of programs.

The operating system identifies the user. During access, he presents an alphanumeric passowrd of up to 13 characters. Access is controlled by using special tables storing information on user rights, i.e. on the authorized operations (writing, reading, updating) on specific files. In addition to tables, user password lists are generated. This is a list of passwords (no more than 64) belonging to one user. After each access, the list is reduced by one. There are also tables delimiting user access to ADEPT from terminals.

Information on magnetic media (cores and drum) is erased especially thoroughly in the system. After processing, information on them is "jammed" with zeros or other characters. A restriction has been introduced on changing user authorities, i.e. a user cannot add to his rights on his own. When necessary, he has to appeal to those responsible for protection and coordinate the new requirements. After obtaining permission, a special program makes the appropriate update to the rights.

Protecting the security of information has been emphasized in the Honeywell global military command and control system for the 6000 series computers. A module has been incorporated in the system that combines facilities for ensuring security: algorithms, codes and tables. They are used to define user and terminal access rules, clear external storage during allocation of it, print security markings, detect breaches of security protection, etc.

To specify access rules, a user security matrix and a terminal security matrix are generated. In the matrices, there is a 23-bit field in which the categories of authorized access and maxmimum levels of security are recorded. The matrices are processed (access is checked) by special program facilities.

During system functioning, the following are provided for: disconnection of terminals, issuing of alarm signals and recording of attempts to breach protection, checking the level of security of information processing results, establishing parameters indicating the security classification of documents to which a specific user has been authorized access, etc.

* * *

Everything written above attests to the great deal of attention paid to questions of designing and incorporating protection systems in computer systems. The framework of a booklet does not permit covering the entire spectrum of experimental developments and operating protection systems abroad. One can, however, assume that highly effective, reliable and inexpensive protection systems will become widespread.

For Those Wishing to Know More ...

BIBLIOGRAPHY

1. Khimerin, D. G. and Myasnikov, V. A., "Avtomatizirovannyye i avtomaticheskiye sistemy upravleniya" [Automated and Automatic Control Systems], Moscow, Energiya, 1979.

2. Shurakov, V. V., "Zashchita informatsii v ekonomicheskikh sistemakh" [Protecting Information in Economic Systems], Moscow, MESI [Moscow Institute of Economics and Statistics], 1979.

3. Bondarenko, V. S., "Sokhrannost' informatsii pri avtomatizirovannoy obrabotke" [Safeguarding Information during Automated Processing], Moscow, Znaniye, 1980.

4. Gerasimov, V. and Vladislavskiy, V., "Hardware Methods of Protecting Information in Automated Systems," ZARUBEZHNAYA RADIOELEKTRONIKA, No 8, 1975, pp 34-46.

5. Stolyarov, G. K., "Review of Proposals by the CODASYL Working Group on Data Bases" in "Algoritmy i organizatsiya resheniya ekonomicheskikh zadach" [Algorithms and Organization for Solving Economic Problems], No 4, pp 48-77.

6. Razmakhnin, M. K., "Physical Facilities for Protecting Computer Centers and Control Complexes," ZARUBEZHNAYA RADIOELEKTRONIKA, No 10, 1980, pp 66-86.

7. Kurmit, A. A., "Data Protection in Multiaccess Systems Abroad (Survey)," IZVESTIYA AN LATVSSR, No 4, 1979, pp 91-105.

8. Kurmit, A. A., "Cryptographic Methods of Protecting Information in Computer Systems," ZARUBEZHNAYA RADIOELEKTRONIKA, No 7, 1979, pp 17-41.

9. "New Equipment for Encrypting Information," ELECTRONICS, Vol 50, No 14, pp 9-10.

10. Martin, J., "Computer Data Base Organization," Moscow, Mir, 1980.

11. Date, C., "Introduction to Data Base Systems," Moscow, Nauka, 1980.

12. Connolly, R., "Standards for Information Encryption Devices," ELECTRONICS, Vol 50, 1977, pp 65-67.

13. "Family of LSI Circuits for Encrypting Digital Information, ELECTRONICS, Vol 50, No 18, 1977, pp 4-5.

14. Hoffman, L., "Modern Methods for Computer Security and Privacy," translated from English, edited by V. A. Gerasimenko, Moscow, Sov. radio, 1980.

15. Walker, B. J. and Blake, I. F., "Computer Security and Protection Structures," translated from English, Moscow, Svyaz', 1980.

16. Knuth, D., "Art of Computer Programming: Semi-Numerical Algorithms," Vol 2, Moscow, Mir, 1977.

17. "Problems of Ensuring Protection of Computer Systems," translated from English, Moscow, Atomizdat, 1975.

Mosaic for the Lecturer

It is of interest to inform listeners that:

...American specialists believe that in the majority of systems now being designed, programs are not thoroughly debugged which causes considerable distortion of information and malfunctions in computer functioning;

...users can be identified by shape of teeth, head and body odor. But the most effective is identification by voice, fingerprints and finger length;

...pasting foil or other magnetic materials on computer center equipment provides for protection against attempts at stealing computer hardware by using a special unit;

...the annual growth in the number of documents in the U.S. Secretary of Defense's Documentation Center is 50,000. And the value of all stolen documents in the United States annually is about one percent of the gross national product;

...modern equipment makes it possible to photograph text on a printer from 70 m;

...over 50 percent of passwords used in computer systems are relatively easy to decode. This is due to their relative triviality; usually used as passwords are autobiographical data--age, last name, place of birth--information describing place of residence (work)--numbers of home and work telephones, houses, apartments, sections;

...using standard methods for erasing information on magnetic media does not completely wipe out the information recorded on them. Special equipment can sense the electrical signals which remain, and after processing, they can be output on a computer printer;

...previously existing highly reliable methods of cryptography did not always permit computing the key used even when the plain text and encrypted text corresponding to it were known. However, by a simple exhaustive search on the top IBM models of, say, 2^{56} keys with a length of 56 bits, the necessary key can be selected within 24 hours;

...to protect information needed in solving problems related to travel on airlines and in space, triple redundancy of computer processors and data files is used;

...Rand Corporation associates, not relying on complex methods of protecting information, consider it expedient though to record attempts at violating and breaking protection schemes. In the firm's opinion, however, a "professional violator' can mask the damage done;

...it seems impossible to determinately evaluate the degree of data protection in functioning computer systems. The ambiguity of an evaluation comes from its probability nature: The majority of factors affecting the degree of protection are random in nature;

...to enhance the conscientiousness of users receiving classified information from a computer system through software, the documents output on a display or printer are assigned a security classification. And for documents kept in one file, the highest classification is assigned.

...the most sensitive protection systems uniquely identify users connected to a computer through terminals by the rate of operation on the keyboard;

...attempts by foreign code-breakers during World War II to break Soviet military and diplomatic codes were fruitless;

...malfunctions in a protection system during normal operating conditions, i.e. when there are no attempts at breaching security and integrity, may go undetected for a long time. Especially complex is the detection of single malfunctions and, consequently, protection against them;

...studies on methods of encrypting information are being kept confidential. American specialists believe that since World War II only three works on this subject with any value have appeared in the open literature. Other works include "revived ideas of antiquity";

...in the data base protection system proposed by the Institute of Standards for future data base management systems in the United States, users are fined for not following the prescribed rules for interacting with certain information;

...In England, a bill on the control of personal information was not approved by parliament. The bill's supporters believe parliament's disapproval was due to the undesirability of reducing the freedom of private enterprise;

...when the coefficient of multiprogrammability is high, the system for replacing keys for protecting areas of main storage should be developed by hardware rather than software.

Attention, Practice ... [insert on pp 32-33]

According to Stanford Research Institute data, in identifying 4,000 people by four fingers, the probability of error was 0.5 percent with a length measurement accuracy of ±1.5 mm.

The IBM Research Center in Zurich has developed a new method of information transmission between various computer devices within a computer center. Data is transferred by using infrared radiation, thereby eliminating the possibility of connection to lines linking a terminal to a computer.

A Siemens transceiver unit is capable of requesting data and entering instructions into a computer without wires within a radius of 20 m. The unit is fastened to the ceiling of a computer center and senses directed and undirected infrared radiation.

The SEKUTRON 5100 (FRG) general-purpose protection system allows arbitrary installation of protective sensors and monitoring system operation automatically (a central unit in the system periodically reports on system readiness and working order). Functions include signalling on toxic gases and flooding, and enclosed protection of sites against break-in and penetration.

Combined application of infrared systems for protection allows the MESL SPACEGUARD IR 733 and 734 to detect motion by people in 18 zones at a distance of 10 m and in corridors up to 35 m long. A parabolic mirror is used to record their remperatures.

The contacting parts of inertial sensors made by INERTIA SWITCH are coated with gold for greater reliability and long service life.

The SIGNAK system automatically analyzes signatures of those entering a computer center. Visitors register by a special pen on a special form. Analysis is performed not on the graphic form of the signature, but on its dynamics: the relationship between time, pressure and angular rate of writing. Reliability is 3.5 percent errors over several years of operation.

Differences in the "acoustic sound" of the body are used in a system, developed by NOVAZ ELEKTRONICS, to organize pass checkpoints. Signals sent by acoustic radiation are reflected from the body, sensed and processed on a computer where "sound profiles" of personnel are stored. Surprisingly, even twins have different acoustic sound.

In the COLLINS CR-100 device, an LSI circuit assembled in a package with 40 pins stores a standard algorithm for encoding information. The code key is entered in the hexadecimal format on thumbwheel switches located under a cover with a lock. The device is made in a desk or rack version and weighs 6 kg.

Protection of information on external storage units has been implemented in the VM/370 virtual computer system and functions of the base computer have been retained.

The standard adopted in the United States for scrambling information calls for conversion of blocks of source information with a length of 64 bits by using a 56-bit key into encoded text by 256 methods. Since the standard was adopted in 1977, there have been no reports on unauthorized decoding of information.

Foreign specialists believe that protection against high voltages penetrating into communication equipment through the main and remote feeding of a circuit with cable multiplex circuits should be implemented by using a cascade protection circuit.

An effort has been underway at Chicago University's Computer Research Institute to develop a protection system with its special class of machine operations. They perform direct hardware processing of requests for the right to use information kept in computer main storage. Further development of the system calls for similar protection of information on magnetic drums and disks.

In the TELECRYPT system made by AEG-Telefunken, the key is generated in the form of a series with a period of about 10^{39} bits. TELECRYPT is made with integrated circuits installed on printed boards and has a built-in check to protect against erroneous transmission of unencoded data.

In Honeywell's MULTICS system, passwords are generated by a computer. A random word generator forms syllables easy to pronounce and combines them into words of varying length. These words are difficult to uncover, easy to remember and convenient to use.

Hitachi's central research laboratory has built a descriptor system with a hardware-implemented mechanism for protection zones. The method was used by BKK for the BKK-500 computer.

8545
CSO: 8144/1695

- END -